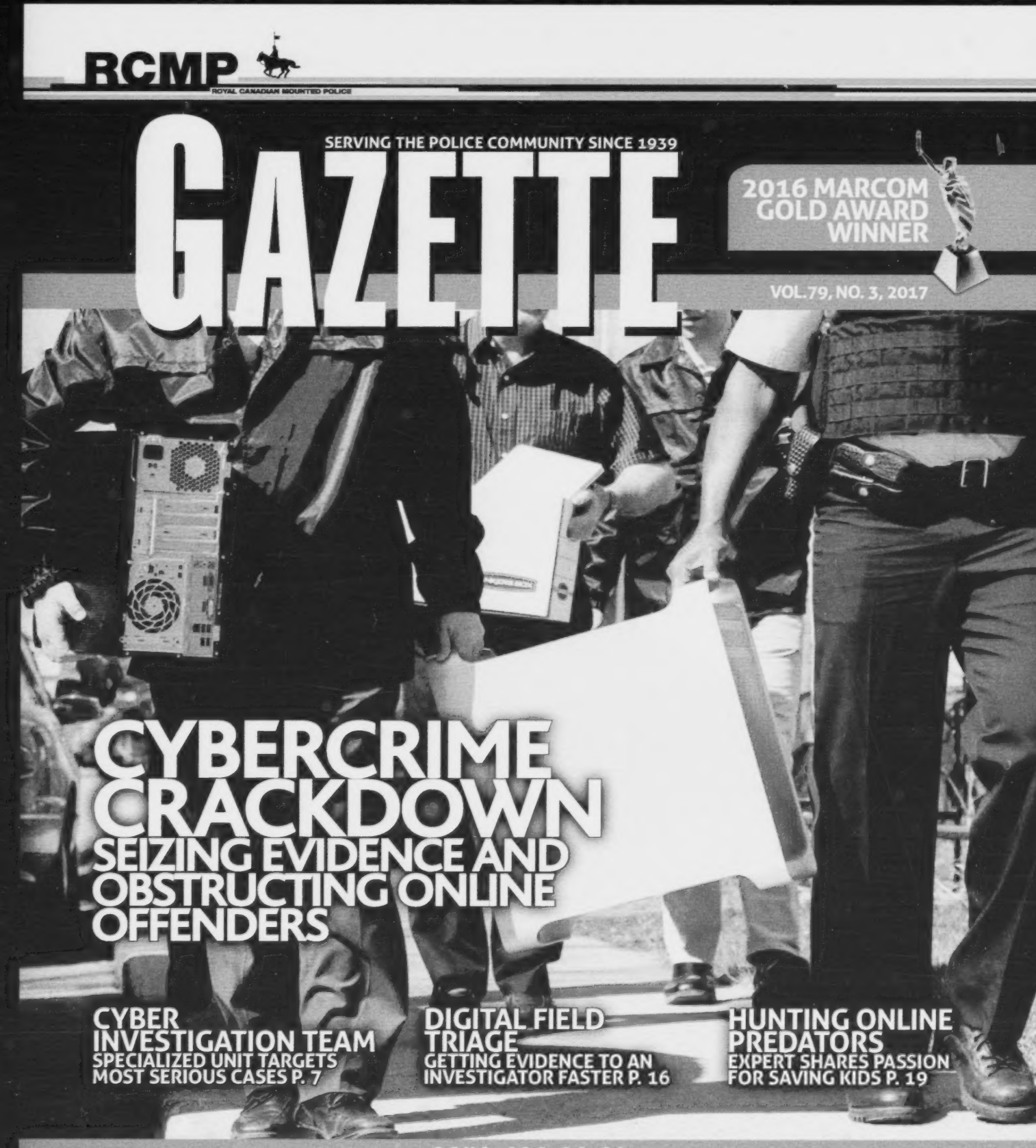
RCMP
ROYAL CANADIAN MOUNTED POLICE

GAZETTE

SERVING THE POLICE COMMUNITY SINCE 1939

2016 MARCOM GOLD AWARD WINNER

VOL.79, NO. 3, 2017



CYBERCRIME CRACKDOWN
SEIZING EVIDENCE AND OBSTRUCTING ONLINE OFFENDERS

CYBER INVESTIGATION TEAM
SPECIALIZED UNIT TARGETS MOST SERIOUS CASES P. 7

DIGITAL FIELD TRIAGE
GETTING EVIDENCE TO AN INVESTIGATOR FASTER P. 16

HUNTING ONLINE PREDATORS
EXPERT SHARES PASSION FOR SAVING KIDS P. 19

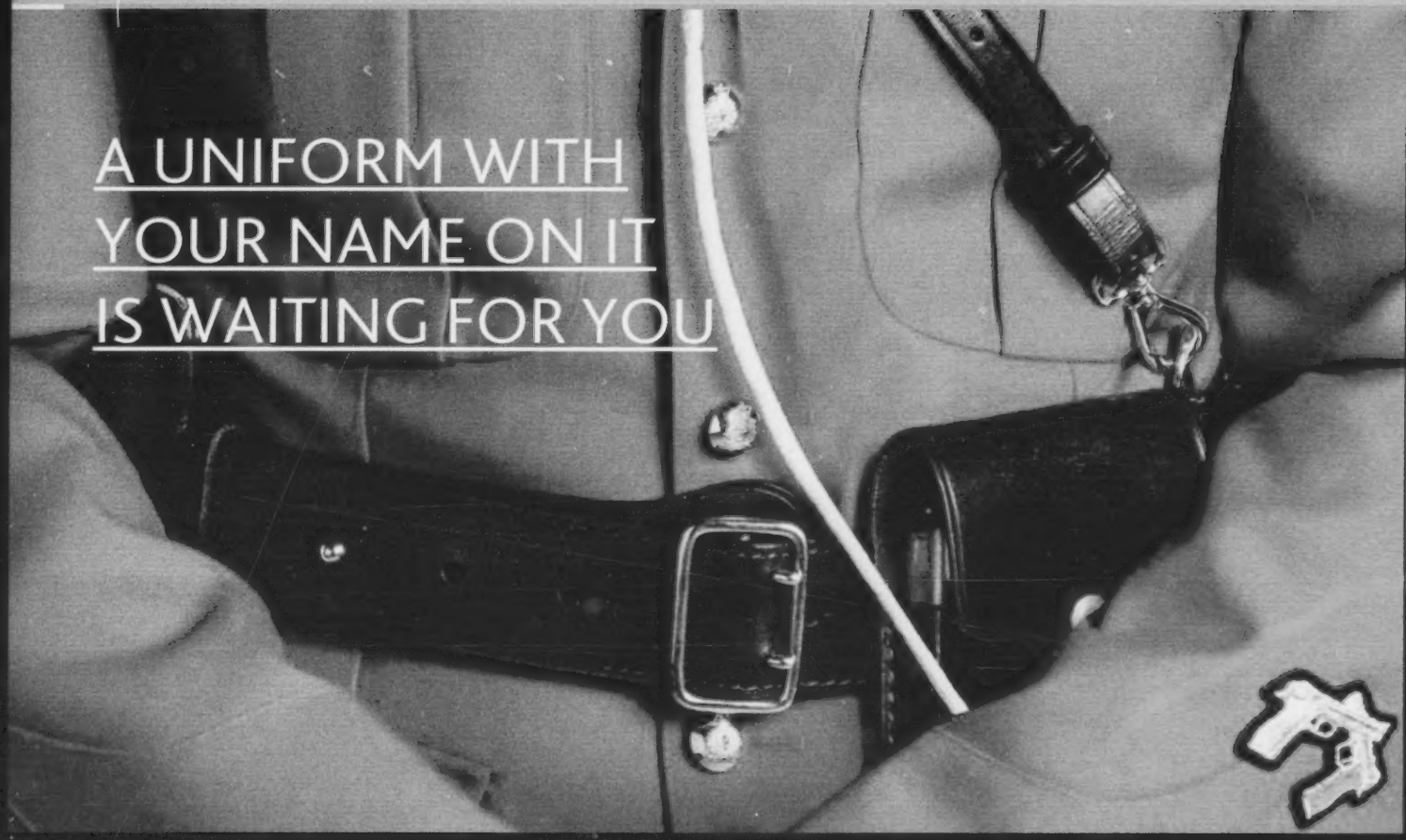
RCMP-GRC.GC.CA

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada

RCMP

ROYAL CANADIAN MOUNTED POLICE



BE READY FOR ACTION FROM THE DAY YOU GRADUATE

Once you've graduated from the Royal Canadian Mounted Police Academy, you immediately start your career in policing.

rcmpcareers.ca

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

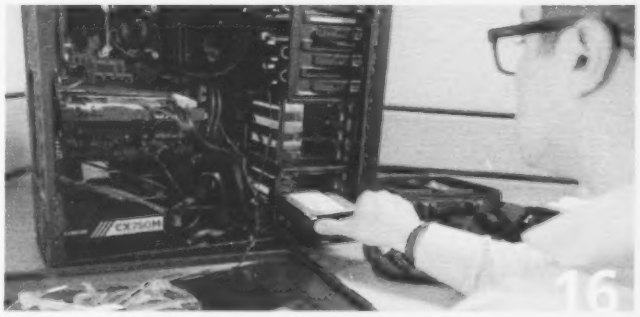
GAZETTE
Serving the police community since 1939
Vol. 79, No. 3, 2017
A Royal Canadian Mounted Police Publication

COVER SECTION

7 Cybercrime investigation team targets most serious online cases
10 How digital forensics specialists make sense of digital data
12 Panel Discussion: What's the greatest challenge in policing cybercrime?
14 Cyber intelligence team gathers information to support investigations
15 Courses teach police how to investigate cybercrime
16 Digital field triage leads to meaningful evidence, faster
17 Workshop helps front-line officers better understand technology
18 New Technology: RCMP seeks software to identify exploitation images
19 Q&A: Covert communication expert hunts online predators

DEPARTMENTS

4 Editorial message
5 News Notes
20 Just the Facts: Auto theft
21 Ask an Expert: Analyst makes sense of communication data
22 Emerging Trends: Policing as a second career
23 Best Practice: Stopping unsafe ATV use in its tracks
24 On the Leading Edge
26 Last Page: Overcoming adversity



ON THE COVER:
Technical know-how and solid investigation skills make a formidable foe for online criminals. Photo: Serge Gouin, RCMP

GETTING CYBER SMART

Serge Gouin, RCMP

The recent global ransomware cyberattack that affected hundreds of thousands of victims as this issue was being finalized highlights what police agencies already know: cybercrimes are increasing in number and escalating in severity.

In 2015, the RCMP launched its cybercrime strategy to fight this threat with a renewed focus on reducing the risk, impact and victimization of cybercrime across Canada.

In this issue, we explore how the RCMP is policing to keep up in this digital era.

For our cover story, Deidre Seiden follows the RCMP's Cybercrime Investigative Team in Ottawa as it advances an investigation it's been dissecting for months. Seiden describes how this new unit works and fits into the bigger picture, nationally and abroad.

Investigations are only as good as the intelligence that informs them. The RCMP's National Intelligence Coordination Centre created a cyber-intelligence team to gather information and identify cyber-related operational opportunities for investigative teams. The team targets hackers and the digital trail they leave behind.

Seiden also examines the digital forensics side of cybercrime and learns how members of the Technological Crime Units across Canada support these investigations by seizing and processing digital evidence. Their expertise is critical when technology can change in the blink of an eye.

And as technology becomes so readily accessible to more people, including criminals, demand for specialty tech units rises exponentially. One way to manage the workload is through digital field triage, a program developed by the RCMP in British Columbia. The program trains non-specialists to determine if a digital device has evidence on it before it's sent for time-consuming analysis. Field triage is getting meaningful evidence into the hands of investigators more quickly.

While not everyone can be a techie, front-line officers need to keep up with the technology, and the laws that govern it. Amelia Thatcher writes about the Cybercrime Investigations Workshop in Nova Scotia — a crash course in Internet and technology crimes. The one-day workshop gives officers the knowledge and step-by-step tools they need when faced with a cyber or technical case.

Identifying child exploitation material and stopping online predators is a monumental task and, when it comes to active abuse, prompt action is critical.

The RCMP is turning to artificial intelligence technology to scan millions of unknown photos and find the ones with the highest probability of being illicit — those digital needles in a haystack. The algorithm can rapidly eliminate images that aren't exploitative and move the most likely to the top of this list. This not only saves time, but reduces officers' exposure to graphic content.

While technology is being developed to take over some tedious and difficult tasks, other methods still rely on the human touch. Thatcher also speaks to Cpl. Jared Clarke, an expert in covert communication, who poses as potential victims or online abusers. His intervention has saved dozens of young victims from further abuse.

This issue isn't just about keeping up with society's rapid migration online. It's about policing smarter — in a world in which almost everything can be done through a computer or a smartphone. ■

— Katherine Aldred

GAZETTE

PUBLISHER: Nancy Sample

EDITOR: Katherine Aldred

WRITERS: Deidre Seiden, Amelia Thatcher

WEB PUBLISHER: Richard Vieira

GRAPHIC DESIGN: Lisa McDonald-Bourg

TRANSLATION: RCMP Translation Services

PRINTING: St. Joseph Communications

The *Gazette* (ISSN 1196-6513) is published in English and French by the National Communication Services of the Royal Canadian Mounted Police in Ottawa. The views expressed in any material published in the magazine or in its online version are those of the authors and do not necessarily reflect the official opinion of the Royal Canadian Mounted Police.

Cover design and contents are copyrighted and no part of this publication may be reproduced without written consent.
Canada Post Publications Mail Agreement 40064068. The *Gazette* is published four (4) times a year and is issued free of charge on a limited basis to accredited police forces and agencies within the criminal justice system. Personal subscriptions are not available.

The *Gazette* welcomes contributions, letters, articles and comments in either official language. We reserve the right to edit for length, content and clarity. © 2017 RCMP.

HOW TO REACH US:

RCMP *Gazette*
73 Leikin Drive,
M8 Building, 1st Floor, Room 801
Ottawa, ON K1A 0R2
CANADA

Phone: 613-843-4570
E-mail: gazette@rcmp-grc.gc.ca
Internet: www.rcmp-grc.gc.ca/gazette

STAY CONNECTED WITH THE RCMP

Visit our website:
www.rcmp-grc.gc.ca

Follow us on Facebook:
www.facebook.com/rcmpgrc

Follow us on Twitter:
@rcmpgrcpolice #rcmpgazette

Watch us on YouTube:
www.youtube.com/rcmpgrcpolice

NEW RADIO SYSTEM ENHANCES PUBLIC SAFETY

By Deidre Seiden

In New Brunswick, speaking in code over the police radio was standard operating procedure for police officers. It was necessary to protect the privacy of calls from people listening in on scanners.

"We thought we were fooling people by having 10-codes," says S/Sgt. Jamie Melanson, a watch commander in the Codiac region. "Everybody knows what 10-4 is. You can look up police 10-codes on the Internet. There's no secret now."

To get around this, dispatch started sending calls electronically, which worked, but only if members were in their police vehicles where they had access to their computers.

The solution was a new radio system.

After working with the provincial government, police and other first responders in New Brunswick have started using the trunked mobile radio communication system (NBTMR). Implementation began early in 2017 and will continue to roll out across the province in stages throughout the year.

"We need to rip out every old radio from the cars, the detachments, everywhere," says Shawn Vautour, director of the Operations Communication Centre and radio renewal project. "It's a significant task but well worth it."

The new system is completely digital and fully encrypted. Police officers can ditch the old 10-codes and speak in plain language.

Vautour says, in addition to this, they're breaking down the communication barriers within the RCMP, between neighbouring provinces and between partners because the systems are all connected.

"It's very exciting," he says. "It works like a cellphone. You could be in the northernmost part of the province and something is happening in the southernmost part of the province and you can still talk to each other. RCMP can talk across borders, from New Brunswick to Nova Scotia to Prince Edward Island. You can have situational awareness."

And for the first time in the province, police can communicate with other provincial first responders.

RCMP

The RCMP in New Brunswick are rolling out a new radio system across the province that's completely encrypted and enhances interoperability between partners and provinces.

"It keeps coming back to public safety," says Melanson. "Something as simple as enhanced communication between agencies enhances public safety because we're all on the same page when we respond to a call together. All I can see is the benefit of this new system." ▪

HELP RICHMOND RCMP IDENTIFY FACES

By Amelia Thatcher

Richmond RCMP is encouraging residents to "get their sleuth on" with the launch of its new website, Richmond Help Identify. The webpage features images of persons of interest that the police have been unable to identify.

With the hope of closing some cases, the detachment is appealing to the community to see if they recognize any faces.

"As police officers, we don't know everybody, so we're hoping that members of the public might connect with a particular image or send it to their friends," says Sgt. Gene Hsieh, head of the Crime Reduction Unit at the Richmond detachment. "The idea is to tap into social media and the local desire to solve crime."

The website is updated regularly with new photos from property owners' surveillance footage, and has even expanded to include composite sketches. For each person of interest, the site also lists what type of crime they may have been involved with, the date the image was posted and the gender of the suspect.

If someone recognizes a face on the website, they are encouraged to call or email the detachment with any information.

"One of the most important aspects of police work is to have a lead," says Cpl. Dennis Hwang, a communications officer who helped start the website. "If we have a name, we can go from there. But when you have nothing to go on, you run the case cold."

In the last several years, home surveillance costs have gone down while the quality of video has gone up, a trend Hwang says has inundated his detachment with hundreds of images of criminals. But, police can't always identify the suspect.

"We have a surplus of photos, and before, it was wasted," says Hwang. "This website helps us leverage the public's knowledge and get people engaged to close cases."

Since the website launched in November 2016, the detachment has made three identifications with tips from Richmond residents. The cases are currently under investigation.

Richmond RCMP

To drum up public interest in their new website, Richmond Help Identify, the detachment tweets out any new faces that make the list.

"We don't want any case, big or small, to fall through the cracks," says Hsieh. "Even if we only get one identification — that's one case that wouldn't have been solved otherwise." ▪

DELTA POLICE TRACK FLEEING VEHICLES WITH GPS

By Deidre Seiden

In the Vancouver, B.C., suburb of Delta, criminals can flee from police, but they can't get far.

The Delta Police Department has installed pursuit management technology on eight vehicles in its fleet. Using GPS, officers can now track vehicles that fail to stop for police.

Officers were dealing with a significant increase in the number of fail-to-stop incidents. In 2016, they had 70 such cases where suspects evaded police.

While researching possible solutions, the StarChase Pursuit Management technology caught the department's attention.

"Our number one priority is public safety," says Cst. Andrew Cortes, a project manager for the new technology. "We needed the ability to increase the likelihood of apprehending these drivers and to decrease the risk to the public, the police and also the offenders that's associated with pursuits. This tool will prevent the fleeing drivers from driving dangerously if they know the police aren't following them."

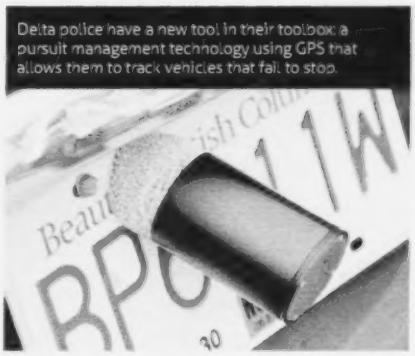
The technology allows police officers to launch a lightweight GPS dart, which is roughly the size of a pop can, from the grill of the police vehicle onto a suspect vehicle.

Once a GPS tracker adheres to the vehicle, police officers can back off, and the Delta police dispatch centre tracks the vehicle and relays updates to the officers.

"This allows our members to come up with a plan for a co-ordinated approach to apprehend the offender once the vehicle is stationary," says Cortes.

Delta police Cst. Jim Ingram was trained to use the new tool and was the first to deploy it operationally. Although the vehicle did stop when he signalled them to pull over, he launched the GPS dart as a precaution.

"If we develop reasonable suspicion that a car might take off on us, someone like a dial-a-doper (drug dealer), we'll tag the car and then attempt to conduct a traffic stop," says Ingram. "Losing bad guys is frustrating. The ability to find bad guys again is less frustrating." ■



Delta police have a new tool in their toolbox: a pursuit management technology using GPS that allows them to track vehicles that fail to stop.

Delta Police Department

MANITOBA RCMP USE PODS FOR REMOTE RESCUE

By Amelia Thatcher

RCMP in two northern Manitoba communities are now using a new rescue tool: off-road transport trailers for stranded residents and criminals.

With exchangeable skis and wheels, the covered trailer pods hitch onto the back of a snowmobile or all-terrain vehicle (ATV) to safely transport up to two people. The bulbous pods resemble over-sized child carriers that are towed behind bikes, with a few added features.

"It's heated, it's lighted and we can use this year-round," says Sgt. Joe Frizzley, the RCMP detachment commander in Thompson, Man. "We're excited to use this for both enforcement and emergency response needs."

The Pas and Thompson, Man., RCMP detachments each purchased a pod last February. S/Sgt. Brent Mattice, commander of The Pas detachment, said the idea came from local emergency services who use a similar pod as an off-road ambulance.

"First and foremost, if someone was ever injured in an isolated area, we can put them right into this pod and take the quickest route we can to safety," says Mattice. "You have a covering — it's totally enclosed so passengers are protected from the elements."

Until now, police used an open sleigh to transport people who were stranded in remote areas. The new pod allows local RCMP to carry injured people more safely, securely and with greater comfort.

Mattice says the pods will also be used to respond to snowmobile and ATV crashes in the bush. Alcohol is often a factor in these accidents, so the detachments needed a way to transport individuals charged with impaired driving.

"The pod has a capability to hold a chair, so if someone is arrested we can safely secure them and bring them back to the office for breathalyzer tests," says Mattice.

Frizzley says the pods aren't limited to carrying people — they can also be used to carry sensitive equipment and electronics to remote crime scenes.

While the pods haven't been used yet, both Frizzley and Mattice agree this will be an integral tool for their units.

"We do have scenes that are in the middle of nowhere," says Frizzley. "Especially in the North, it gives us an avenue to get our people out safely." ■

The new pods can be towed behind snowmobiles in the winter and, in summer, the skis can be changed for wheels and towed behind all-terrain vehicles.

Cpl. Colin Stark, RCMP

Serge Gouin, RCMP

The Cybercrime Investigative Team is dedicated to combating pure cybercrime that impacts Canada's government and critical infrastructure.

MANY SKILLS, ONE GOAL

NEW INVESTIGATIVE TEAM TAKES ON CYBERCRIME

By Deidre Seiden

It's crunch time for the RCMP's Cybercrime Investigative Team (CIT). It's Friday and the last working day before the team travels out of town to execute a search warrant and arrest a suspect in their latest investigation.

*Cst. Falardeau drops in to see *Sgt. Beaulieu, the CIT's operations noncommissioned officer (NCO), to collect any specific instructions for the courthouse. Falardeau is the affiant responsible for writing the search warrant for the investigation.

"We need to get this search warrant signed by a judge today," Falardeau says. "This is a critical piece of the puzzle."

Members of the team have been stopping by Beaulieu's desk in a steady stream all morning to ask last-minute questions relating to the case.

"This is the exciting part," says Beaulieu. "For three months we've been doing our due diligence, gathering evidence against the suspect. Now we're ready to arrest him."

NEW STRATEGY, NEW TEAM

For years, the RCMP has been actively prioritizing cybercrime threats, investigating and interrupting cybercrime activities and handling digital evidence in support of investigations, but the CIT is the first team dedicated to investigating pure cybercrime in Canada.

Located at the RCMP's National Division in Ottawa, this highly specialized team was created in 2015 to investigate crimes where the computer or the technology is the target.

Its creation was a key step in the RCMP's cybercrime strategy to reduce the threat, impact and victimization of cybercrime through enforcement.

"They're the sharp end of the strategy," says Supt. Denis Desnoyers, the criminal operations officer for National Division.

While many countries have had similar dedicated investigative teams for several years, Canada is in a good position to benefit from the lessons learned.

"You might not go through the growing pains that other units have gone through because you don't have to reinvent the wheel," Desnoyers says. "As a result, our team has quickly gotten up to speed."

Traditionally, the RCMP's Technological Crime Units (TCUs), which are located across the country, have had the responsibility of investigating cybercrime. However, because of the workload of most of TCUs, this was rarely the case. Their priority has been supporting investigations conducting digital forensics.

With the creation of the CIT, the team has taken over the most serious cybercrime files. The nature of the files they handle lend themselves to high-profile cases that have an international component, are sensitive in nature, affect critical infrastructure or target federal government infrastructure.

S/Sgt. Maurizio Rosa is the NCO for the Technological Crime Unit at National Division. The CIT falls under the umbrella of the TCU, which also holds the Digital Forensics Team.

Rosa has been instrumental in building the team from the ground up. From the beginning, he had a clear idea about what he wanted it to look like based on his experience working general investigations and as a digital forensics investigator.

His goal was to get a good mix of technically knowledgeable investigators as well as sound traditional investigators.

With that in mind, he selected applicants based on their backgrounds, evaluated them and built a team with complementing skillsets.

There are two sides of the team: the investigative side that does the traditional police work related to cyber offences, and the digital forensics side that processes digital data in support of the charges.

"It's been a successful model," says Rosa. "The team that's being built right now has a very strong morale, has a very good work ethic and has dedicated and initiative-prone members."

Now in its third and final year of implementation, the team has reached a point of critical mass. For this new team, the current investigation is one of the first in which charges are imminent.

BRIEFING

Just before 10 a.m., Beaulieu heads down to the boardroom for the final briefing in Ottawa and takes a seat at the conference table.

The pressure might be on, but the atmosphere in the room is relaxed as members of the investigative team wait for the briefing to begin.

The lead investigator on the case, *Cst. Veilleux, walks in and captures the room's attention.

He goes over the project details, listing the activities the suspect has been under investigation for, who he's known to associate with and where he's been known to go for dinner, urging members to avoid those places.

Every detail has been dissected.

"There's no room for error in an investigation like this," says Veilleux.

Not only is cybercrime investigation a newer area for the RCMP, it's a relatively new area in jurisprudence and case law. There are few cases that have met the test of the courts.

"We have a big responsibility," says Rosa. "We have to be confident in the investigative techniques that we employ but still mindful of doing it in such a way that will withstand the scrutiny of the courts."

Veilleux goes over a long list of items to seize, including computers, laptops and cellphones, as well as bank statements and documents related to specific websites.

He can't say for sure how many computers and cellphones the suspect has. He does know that the suspect posted a device online to sell.

"Did we try to buy it?" someone asks, getting a laugh from the room.

Finally, Veilleux tells the team that their safety is his number one priority. "We're all going in together. We're all coming out together."

It's a reminder that there's always a risk involved, even with cyber operations.

BORDERLESS CRIME

Traditional crime, such as a bank robbery, often presents an element of danger. These physical and violent offences pose a high risk to the public, to police officers and even to the criminals themselves.

In cyberspace, an actor can hide behind anonymity.

"Crime on the Internet and cybercrime is on the rise," says Rosa. "When there's ever an opportunity for a criminal to reduce their risk and increase their reward, they are going to take it."

While they may not know their victims personally, the scope and impact of their actions can be detrimental at the individual level as well as at the national or even global level.

"When you look at computer data and cybercrime, it doesn't see borders," says Beaulieu. "It can travel just about anywhere."

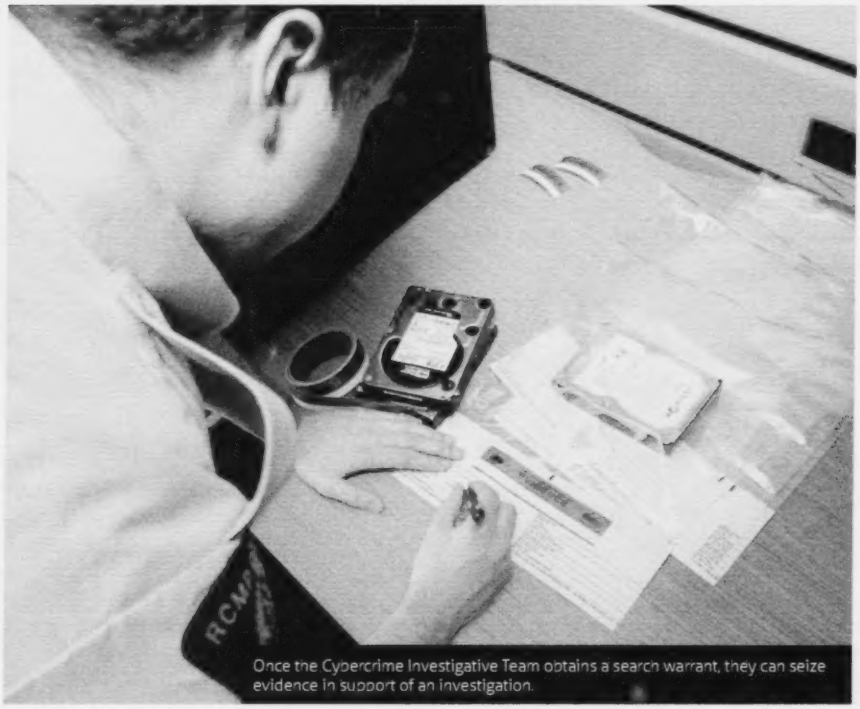
Combating cybercrime often requires collaboration between multiple police agencies, both domestic and international.

Criminals have the luxury of not having to deal with judicial authorizations or within the confines of the law. Nor do they have the same budgetary restraints and resource restraints as police agencies.

"We're dealing with concepts that are extra-jurisdictional, where we may have to get evidence from another country, where the criminal may be located in another country or where a Canadian criminal may be attacking another country," says Rosa. "So we often work with our partners to share information and on joint investigations."

The RCMP takes an intelligence-led approach to policing, which includes intelligence gathered by domestic and international partners. In this case, the suspect gained the attention of a policing partner, who brought the case to the RCMP.

After spending three months investigating the suspect, the CIT had enough



Once the Cybercrime Investigative Team obtains a search warrant, they can seize evidence in support of an investigation.

Serge Gouin, RCMP

evidence to demonstrate to a judge there was reasonable grounds to obtain and execute a search warrant.

ON THE ROAD

And with that in hand, they are ready to make their move. While the team is based out of Ottawa, the crimes it investigates are scattered across Canada.

"I wonder what he [the suspect] is going to think tomorrow when we knock on his door?" says Veilleux.

There are still several details to go over when they arrive at their destination, such as how they'll enter the residence.

As carefully thought-out as their plan is, there are still things they can't control, including whether the suspect will even be at home. The suspect isn't currently under surveillance.

"He has to be at home," says Veilleux. "He always sleeps in his own bed ... if he's not there, we'll deal with it and still do the search."

When everyone has reached the hotel, the team meets once again. The 10 people who make up the RCMP contingent plus a few others from partner agencies crowd into a small hotel room.

They confirm their plan for entry — to knock and wait for the suspect to answer, and only do a forced entry if necessary.

"We're going to have to be flexible tomorrow," says Veilleux. "I can run through a whole bunch of scenarios, but we'll have to go with the flow. See you in the morning."

TAKEDOWN

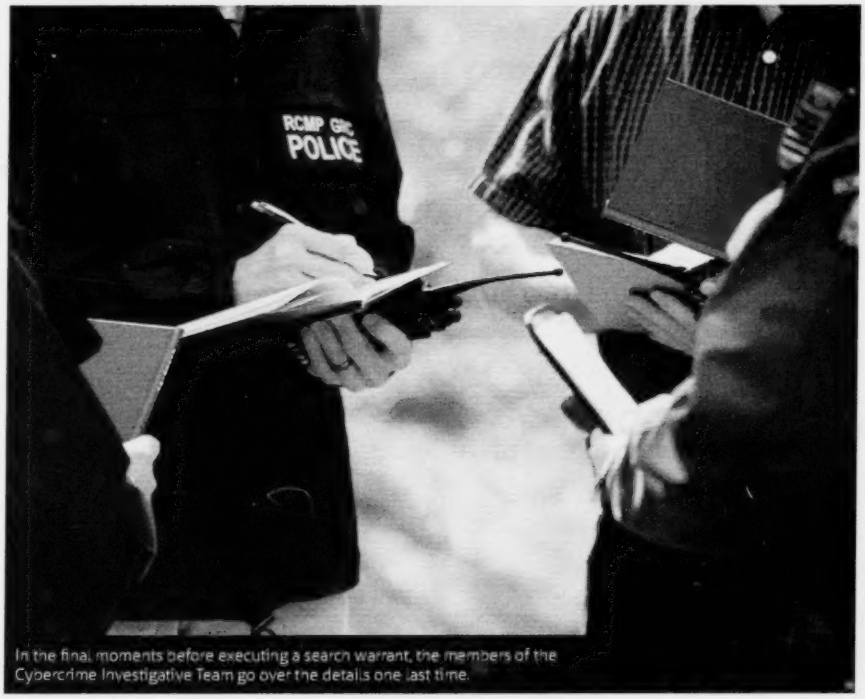
All the work they've done so far has led toward this moment. The operation is the culmination of meticulous research, good investigative techniques and persistence.

"Building concrete evidence in these types of cases is particularly challenging," says Rosa. "We can't just decide tomorrow that we're going to go execute a search warrant somewhere. Just being able to get to that threshold is quite hard."

The team has gathered in a parking lot a short drive from the site. With most dressed in plainclothes, with their soft body armour and firearms under their jackets, the only thing that identifies them as police are the two officers with them dressed in uniform.

After one final huddle, they get into their vehicles and drive to the suspect's residence.

The two civilian digital forensics analysts remain behind. They won't enter the home until the suspect has been arrested and the house has been cleared.



Serge Gouin, RCMP

In the final moments before executing a search warrant, the members of the Cybercrime Investigative Team go over the details one last time.

"We're usually the last ones in and the last ones out," says an *analyst with the TCU. He's technically on the Digital Forensics Team, but often members from the two teams cross-pollinate.

As computers, cellphones, USB keys, even burnt CDs are found, the digital forensics investigator and analysts will process the data on site to determine if it needs to be seized.

Processing it on site can save them time later on. Everything that's taken must meet the criteria of the warrant and becomes the responsibility of the RCMP.

About an hour later, the analyst and his partner receive word: the suspect has been arrested. It's the best case scenario — everything went smoothly.

The suspect is detained and brought to a local RCMP detachment. He is later interviewed.

The investigator conducting the interview, *Cst. Poulin, has a specific approach in mind.

"I've done the research as to what evidence we have against the suspect," says Poulin. "I think any interviewer, no matter the type of file, will do their research beforehand if they can. If you know the suspect's interests and background, you can draw a bit more from them. In this case, we had a lot of background information on the suspect."

With the suspect seated at the table, Poulin puts his strategy in motion. Over the next few hours, he establishes a friendly rapport with idle chit chat. Then he starts asking the suspect some basic questions about what he does.

Poulin builds on every answer, applying pressure and easing off when he needs to keep the conversation going.

In the end, the strategy worked — Poulin obtained a confession.

Back at the house, the search warrant also went well. They didn't encounter any digital roadblocks and were able to collect what they needed.

It's been a long day, but a good one.

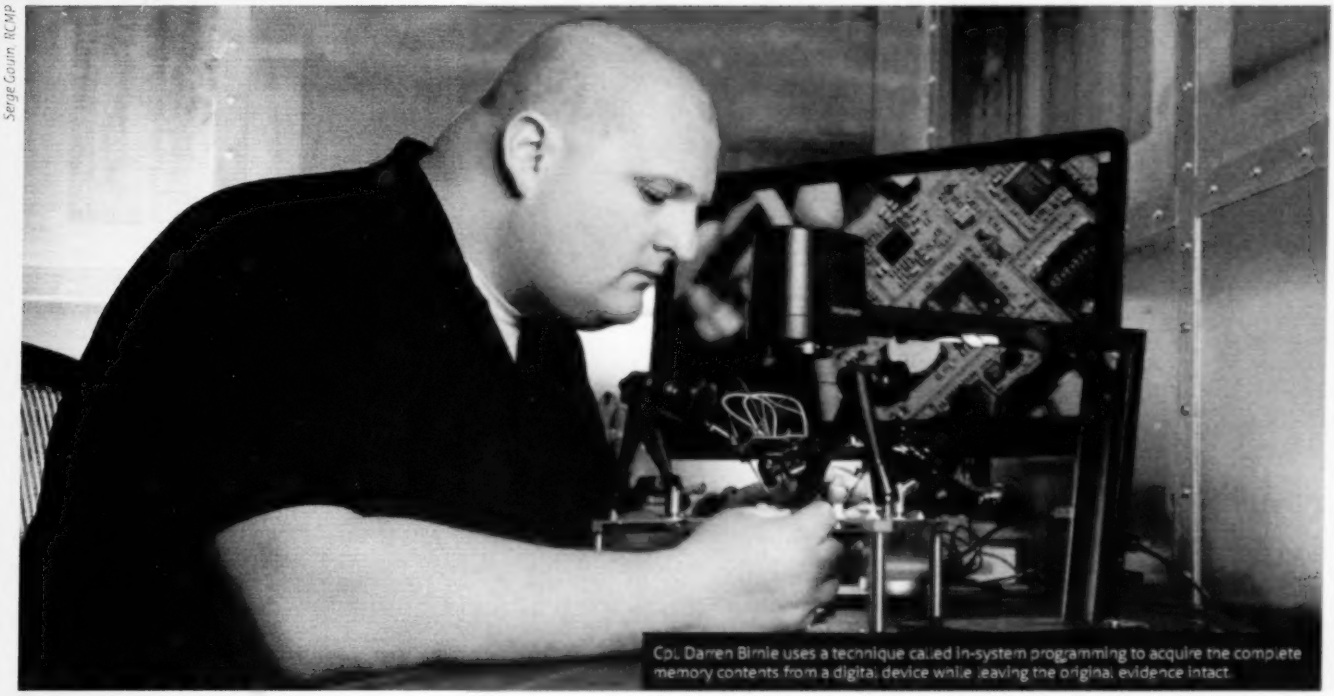
ONE STEP CLOSER

Beaulieu is pleased with his team and the results that their careful planning has yielded.

"We got everything we were hoping for and then some," he says. "Our ultimate goal is to identify crime, investigate and then hopefully we're successful in identifying the perpetrator and bringing him to justice. We're one step closer to that now."

**Some names are being withheld for security reasons.* ■

Serge Gouin, RCMP



Cpl. Darren Birnie uses a technique called in-system programming to acquire the complete memory contents from a digital device while leaving the original evidence intact.

BEHIND THE SCREEN

DIGITAL FORENSICS SPECIALISTS UNCOVER, INTERPRET DATA

By Deidre Seiden

In the office of the RCMP's Technological Crime Unit (TCU) at National Division in Ottawa, a small request to open a USB key has turned into an animated discussion about protocol and process.

In the field of digital forensics, preserving the integrity of data on a device is a key component of their work. It's crucial that members of the unit know all the facts before they access electronic data. So when a colleague from another team asks if digital forensics can take a look at the content on the USB key, the unit has questions.

What is it? Where did it come from? The simple act of opening the files could have negative consequences.

"We need to make a forensic copy of that USB to preserve the original content," says Sgt. David Connors, the non-commissioned officer in charge of operations for the Digital Forensics Team within the TCU. "For evidence to be admissible in court, we have to prove the evidence is the same piece that was taken at the scene. You can't say it's the same piece of evidence if for the last year everybody and their brother has been manipulating it. Any change that we do make to a device, we document."

In addition to preserving evidence, digital forensics specialists also perform a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events. Essentially, they make sense of this type of evidence so those without the high-tech background can understand it.

DIGITAL DATA

It's not hard to see why digital forensics investigators (DFI) and analysts are often referred to as the techies by the clients they support. Their work with computers, cellphones and computer networks — anything related to digital data — would make most people's heads spin.

"It's very challenging work," says Cpl. Darren Birnie, a DFI with the TCU. "It's a very exciting career path if you're into continuous learning and new challenges all the time. When I start looking through these systems, you never know what you're going to get and I've been doing this since 2009."

The technology rapidly changes.

"We have to adapt constantly," says a civilian analyst with the TCU. "New cellphones come out every few months. Today we're doing something one way. Next month you might not do the same thing to get the same result. We have to keep up and research all the time."

But while the unit must remain current, the investigations themselves are complex and can take time. The TCU in Ottawa was involved in investigating the Canada Revenue Agency Heartbleed hacking case in 2014. On May 6, 2016, the individual, Stephen Solis-Reyes, pleaded guilty to two counts of willful mischief (data), one count of unauthorized use of a computer and one count of obstructing a peace officer.

For the past few months, Cpl. Sébastien Laurendeau, a DFI with the Cybercrime Investigation Team (CIT), which is integrated with the TCU, has been spending his days searching data on hard drives, trying to find

evidence to connect a suspect to the offence. While patience is required, Laurendeau says the work is satisfying.

"It's rewarding when you're able to connect the dots," says Laurendeau. "Even just figuring out how things work, 'Oh! This is how he was doing this.' When you're able to see that you're progressing and getting somewhere, it's fun."

LEARNING THE ROPES

Before joining the CIT, Laurendeau didn't consider himself to be a techie. His interest in digital forensics began with an online luring case he worked on when he was doing general duty in New Brunswick. He called the TCU in New Brunswick for advice.

"I tracked down my suspect using IP addresses and dealing with service providers, which got me really interested in it," says Laurendeau. "People think they're anonymous when they're online, but they aren't. I was able to find my suspect, arrest him and he was actually convicted."

This experience led him to pursue a career in digital forensics. He took a few courses to increase his knowledge, then applied. He first joined the TCU in New Brunswick before becoming a member of the CIT in Ottawa.

While several members on the TCU have a background in computers, it isn't necessary. There's an understudy program for successful candidates, which includes a combination of computer forensic courses at the Canadian Police College and on-the-job mentoring by a coach.

It typically takes one to two years to complete before DFIs are ready to work independently, which means there's a long time between hiring someone and having them work on their own.

GROWING FIELD

Based on the tools and state-of-the-art equipment the team has at their disposal, like the multi-million dollar server room to protect them from malicious attacks, it's clear the unit is a priority for the RCMP.

There's a TCU in every province to support local detachments. These provincial units see more street-level files, like assaults, break and enters, thefts, frauds and domestic disputes, but they also support major investigations involving homicides, large frauds, drug trafficking, organized crime, border/customs and national security.

The TCU in Ottawa differs in that it primarily supports larger and longer investigations, generated by National Division's Sensitive and International Investigations that examines political files, corruption, breach of trust, war crimes and kidnapping. The unit also supports National Capital Region Traffic services, General Duty Protective Policing, VIP, Prime Minister's Protective Detail and the Governor General's Protective Detail. And because the Ottawa TCU is integrated with the Cybercrime Investigation Team, they support cybercrime files as well.

Almost all investigations now involve some element of digital forensics. "Realistically, every single case could have a digital component," says Birnie. "But also realistically, there's a finite amount of resources so there has to be a cut off on what we can invest time in and what is not necessary for prosecution to take the case to court and be successful. There are just not enough tech crime guys to go around."

Connors says this means there's a continued need to develop expertise in digital forensics and push the information to the frontline.

"As more and more average people go to the online world to do their day-to-day business, more and more criminals will move into the same space and more police operations are going to have to take place there, too," says Connors. ■

**Some names are being withheld for security reasons.*

A MOBILE SOLUTION

By Amelia Thatcher

The RCMP's Technological Crime Unit (TCU) in Nova Scotia brings their expertise directly to crime scenes with a unique mobile lab. The non-descript white trailer is brought along when police execute search warrants at any location in the province.

"When we attend a search scene, we're at the mercy of the environment we walk into," says Cpl. Duane Flynn, a forensic analyst at the TCU. "The mobile lab gives us a safe environment to do our work."

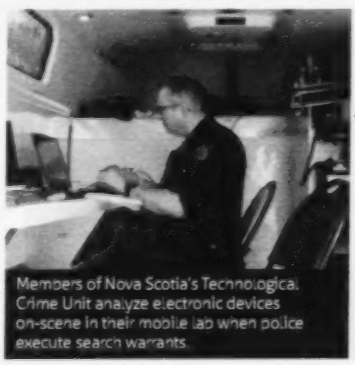
For the last three years, the mobile lab has provided a clean, safe space for analysts at the TCU to do their job.

It has a generator for power, and can fit two analysts at a small desk with a separate bench for two investigators.

"It gives us the capability to go to a scene, pull out the data that's needed and provide it to the investigators immediately," says Sgt. Royce MacRae, officer in charge of the TCU. "It not only saves time but provides a much better product to the investigator. When they leave that scene, they have something to go on when they interview suspects."

Before performing a search, TCU analysts discuss what they'll be looking for with the investigator in charge of the case. They try to narrow down what devices they'll need to search in advance — be it a computer, tablet, smartphone or other digital device. Flynn says his team usually spends about five hours going through digital data on-scene.

"Our goal is to identify what types of devices we need to find to help further the investigation," says Flynn. "Sometimes, it can be a needle in a haystack because of the amount of data we find, but we try to narrow that down as much as possible."



Cst. Todd Bromley, RCMP

Members of Nova Scotia's Technological Crime Unit analyze electronic devices on-scene in their mobile lab when police execute search warrants.

WHAT'S THE GREATEST CHALLENGE IN POLICING CYBERCRIME?

THE PANELLISTS

- **Jeffrey Thomson, criminal intelligence analyst, Canadian Anti-Fraud Centre, North Bay, Ont.**
- **C/Supt. Jeff Adam, Director General, Technical Investigation Services, Ottawa, RCMP**
- **Bessie Pang, Executive Director, The Society of the Policing of Cyberspace (POLCYB), Richmond, B.C.**

JEFFREY THOMSON

Cybercrime is far from being a new phenomenon. Yet, even today, we hear things like "there's no likelihood of arrest", "we won't extradite to Canada", "this is outside of our jurisdiction", "the evidence is in another country" and "we don't have the resources." Are these conclusions indicative of law enforcement's knowledge of cybercrime? Do they reflect our capacity to investigate? Or is it something else?

Some have even said that Canada isn't equipped with laws to investigate extraterritorial offences, despite Section 7 of the *Criminal Code of Canada*, which, "permits some offences to be tried in Canada as if the offence had occurred here."

These challenges are not new. Early assessments and studies on cybercrime (2007 to 2009) identified that as the world became more reliant on the Internet, cybercrime would increase. This research predicted that new technologies, software, malware, security of computer systems, anonymity and jurisdictional issues would pose challenges to law enforcement and that law enforcement would need more capacity to investigate these crimes. And yet here we are today, almost 10 years later, and we're still hearing about the same issues.

So, what's at the heart of these issues? For many police services, it's capacity and knowledge. Police officers attending to the calls for crimes such as business email compromises or ransomware are expected to investigate, collect statements and evidence for crimes that many have never dealt with and often don't understand.

And even when they are able to pull together a good file, many are left saying "now what do we do?" The money went to another country, the emails or fake websites are hosted in another country, the illicit drugs seized were purchased on the Dark Web, or even the criminals are located in another country.

Do police in Canada have the tools and powers to go after the perpetrators? And would they have the support of the already over-tasked public prosecution system, one that many officers consider too lenient when it comes to punishing cyber thieves, fraudsters and other criminals, and one that is likely also suffering from the same challenges of dealing with cybercrime?

In 2014, the Government of Canada enacted the *Protecting Canadians from Online Crime Act* (Bill C13). Considered by some as Canada's response to implement obligations to *The Budapest Convention on Cybercrime (2001)*, Bill C13 was adopted to increase the power of law enforcement in their investigation of online activity. But again, what does

this mean for policing today? Would a survey of police officers find that they know and understand this new bill?

So perhaps the questions is not what is the greatest challenge in policing cybercrime but rather why has policing cybercrime become so challenging? A typical answer has been provided to the first question: resources and capacity, including knowledge, and training built into every level of policing. As for the second question, this is another philosophical question that could identify areas for improvement, where limited investment could fill some of the intelligence gaps we face today.

C/SUPT. JEFF ADAM

The policing principles that came from Sir Robert Peel in 1829 were established in an era where the victim, the offender and the police/judiciary were all co-located in geography. The first principle — to prevent crime and disorder — was focused on the "localness" of crime and the ability of the police to carry out their functions of preserving law and order.

You can see where this is going. The public contract, which is to maintain order and prevent crime, gather evidence, arrest the perpetrator and bring them to justice, is shattered when the new realities of an interconnected world are considered. When the offender is almost always in another country, the geopolitical boundaries that have served nations well for hundreds of years are irrelevant in cyberspace. And to consider being prescribed by those boundaries would negate the value of the Internet to commerce, education and cultural sharing around the world.

The police culture in Canada today is one that has developed over time: prevent crime, maintain order, gather evidence and present the accused for trial. Much of our resources have been focused on the deliverables inherent in those functions and, where those measures are most easily captured, is in the latter two activities in that list. It's far easier to count and report on offences, arrests, convictions and clearances than it is to report on how many crimes were prevented or how victims were assisted and supported.

But in cyberspace and the crime that's in that space, the ability to arrest the offender and bring them to justice is much more challenging. So if police can't bring the offender to justice, much more effort will move toward crime prevention and victimization, and then this question: are police the most appropriate agency to perform those functions in this new space? I believe that the answers to this will involve a whole-of-society approach, since the traditional and well-practised approach to crime won't be effective in addressing cybercrime. This will not be solved by the police alone.

There are other challenges in investigating cybercrime. Where is the evidence? When an offender hacks into data that is hosted on the cloud, where did the offence take place? And who is investigating?

The Internet has caused an enormous, wide-ranging and profound change in how we live our lives and communicate with each other. How we work together to adapt and respond to the challenges cybercrime brings will change how a community engages to police cyberspace, not how the police do the policing.

BESSIE PANG

In today's digitally connected world, our daily lives are intricately woven into the maze of Internet of Things (IoT), ranging from the use of smart fridges and thermostats, to the smart mattresses that can adjust to improve your quality of sleep. According to a report from Berg Insight, Europe and North America had 17.9 million smart homes in 2015. North America will see 46.2 million smart homes by 2020, comprising 35 per cent of all households.

Consumers are constantly being propelled into the fleet of rapidly evolving smart technologies. While consumers are swift to adopt various smart appliances at home and in the workplace as convenient appendages to their daily activities, they are generally less vigilant against the possible cybersecurity vulnerabilities that could expose them to cybercriminals and hackers.

In general, when considering IoT purchases, consumers are not likely to ask the sales associate whether or not the smart mattress or smart coffee-maker was patchable (software update for fixing security vulnerabilities), yet these are indeed the questions that consumers need to include in search-for-product information.

The risk of cybercrime victimization amongst certain community sectors, such as seniors, immigrants and refugees, is further elevated, due to physical, social, language, cultural and physical barriers in accessing cybercrime awareness information. For instance, a senior with limited mobility could now deploy various medical devices to maintain independent living. Some of these devices could deliver real-time health data to the physician, others could notify a family member by text, email or phone call when the senior skipped a meal. A "smart garment" could even activate wearable airbags during a fall.

Despite the obvious medical benefits, a patient is unlikely to have discussed with the physician how a compromised smart medical device might impact his/her health, particularly during an emergency.

Empowering consumers to make informed decisions, based on the cybercrime risks and benefits of some IoT products, could be life-saving when certain smart devices cease to deliver smart solutions.

As a not-for-profit, international organization, The Society for the Policing of Cyberspace (POLCYB) strives to enhance private-public collaboration to facilitate information-sharing in policies, strategies and good practices in cybercrime prevention, detection and response.

POLCYB also promotes public education on cybercrime awareness. From POLCYB's perspective, the most significant challenge lies in enhancing accessibility to public education information on IoT vulnerabilities in relation to cybercrime risks. Exploring effective service-delivery modes in community outreach strategies is essential.

In addition to the call for private-public partnerships in promoting public education, seeking collaboration from community-based organizations is essential. Organizations and services, such as counselling services, immigrant and refugee settlement services, assisted-living facilities and community centres, could be encouraged to collaborate with law enforcement and industry partners to modify and deliver cybercrime prevention information to better suit the needs of their respective community groups. Once service providers have received proficient cybercrime prevention training, they could, in turn, act as focal points from which information could be passed on informally to their clients.

Public education is an important facet of cybercrime prevention, but law enforcement agencies require support from community groups. Ongoing community capacity-building will become increasingly essential as IoT continues to penetrate into all sectors of our community. ■

INFECTED INTERNET

RCMP CYBER-INTELLIGENCE TEAM TARGETS HACKERS, BOTNETS

By Amelia Thatcher

The Internet has become an indispensible part of our lives — we can use it to pay bills, order food and even find love. But while its use has increased exponentially, so has its misuse by criminals.

"Cybercrime is in everything — every field and industry," says Supt. Marie-Claude Arsenault, officer in charge of the cyber team at the RCMP's National Intelligence Coordination Centre (NICC). "Most crime, whether it's cyber-enabled or cyber-targeted, has an online or technical aspect."

To keep up with society's rapid migration online, the NICC created Arsenault's cyber-intelligence team in 2014 as part of the RCMP's cybercrime strategy. Its mandate is to gather information and identify cyber-related enforcement opportunities for provincial, national and international investigative teams.

"We're proactive in trying to find leads and developing a case to a point that when it's passed onto the division [province or territory], they can get right to it," says Arsenault. "Oftentimes they're so busy they can't spend time searching for the next case, and that's where we come in. We can have something ready for them to pick up, and all the legwork is done already."

Although nearly every police investigation now involves technology, Arsenault's cyber-intelligence team focuses on a very specific area: cyber-targeted crime, where the technology itself is attacked.

"We mainly focus on just two sections of the Criminal Code — mischief to data and unauthorized use of a computer, or hacking," says S/Sgt. Paul Poloz, in charge of intelligence priorities at the NICC. "With other crimes like fraud, child exploitation or compromised emails, the end goal is not the computer or the technology — they just use it as a tool. We focus on pure cybercrime."

The team targets hackers who author or use malicious software (called malware) such as computer viruses. They're tracking the digital trail of these cyber-criminals, looking for anyone who is compromising the infrastructure of the Internet.

ROBOT NETWORK

One of the biggest threats to the Internet — and one of the cyber team's biggest priorities right now — are botnets, or robot networks. Botnets are created when a large number of devices connected to the Internet are compromised and directed to do things they wouldn't normally be doing, usually for nefarious criminal purposes.

A device becomes compromised when it's infected with malware, which infiltrates the computer system without the owner's consent. An infected device becomes hypnotized and can be controlled remotely by cybercriminals.

When creating a botnet, the hacker's goal is not to infect one or two devices, but hundreds of thousands of computers, smartphones, GPSs, routers and anything else that's connected to the Internet. They can direct their botnet to send spam emails, transmit viruses and engage in other acts of cybercrime.

"Cameras and home security systems, even refrigerators that are connected to the Internet — they're not secure," says Greg Simmonds, manager of the NICC's cyber team. "They're sitting there and someone who's skilled and knows how to take control of those things can use them as access points to do criminal activities."

One such criminal activity is called distributed denial of service (DDoS) attacks. In most DDoS attacks, hackers direct their botnets to flood a website with traffic, effectively shutting it down to legitimate users. Motivations for these attacks can include blackmail, taking out competition, or simply expressing anger towards the website's owner.

"Often, you have the victims in one country, the bad guys in another country and the servers in another country," says Arsenault. "You can have three or more jurisdictions involved, which is why it's so hard to police this. It's very important to have international partners when we're dealing with cybercrime."

KEEPING UP

According to Arsenault, demystifying cybercrime worldwide is a major first step in stopping these illegal online activities.

"It scares police forces," she says. "In one jurisdiction, you can have 20 break-and-enters and police will respond. But you can have 20 cyber attacks but police won't do anything. It's not always treated as a crime."

She hopes that educating police will make a difference at various levels, from the frontline to the specialized teams. And while most police forces are still catching up when it comes to investigating cybercrimes, Arsenault says in one respect, the RCMP is at the forefront.

"On the intelligence side, we're ahead," she says. "There aren't too many police forces that have a dedicated cyber-intelligence team." ■

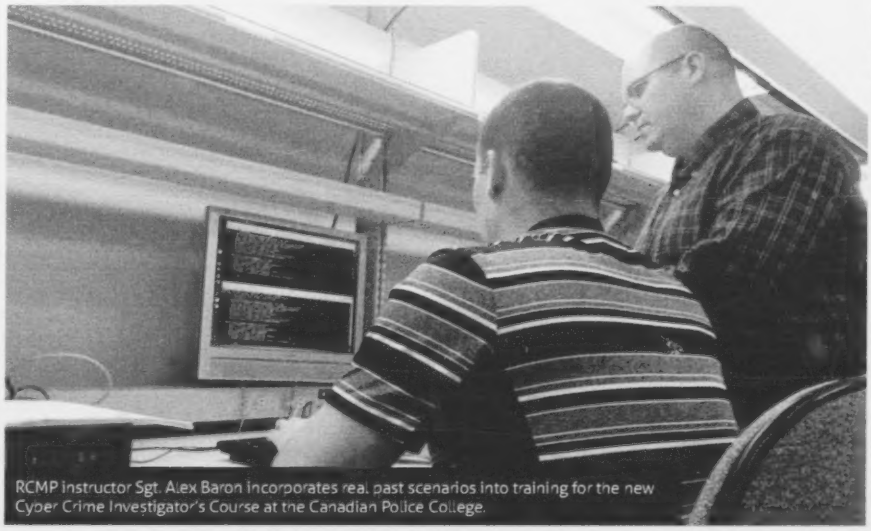
Amelia Thatcher, RCMP

This past April, RCMP Supt. Marie-Claude Arsenault (centre) and police representatives from around the world shared best practices on how to combat cybercrime during the International Cybercrime Operations Summit.

SHARPENING CYBER SKILLS

COURSES TEACH POLICE HOW TO INVESTIGATE CYBERCRIME

By Amelia Thatcher



Courtesy Sgt. Alex Baron, RCMP

RCMP instructor Sgt. Alex Baron incorporates real-past scenarios into training for the new Cyber Crime Investigator's Course at the Canadian Police College.

On the Internet, criminals are shrouded in anonymity, making cyber investigations a difficult task for police. The Canadian Police College (CPC) in Ottawa is trying to stay one step ahead of those cyber-criminals by adding a new course to their arsenal: the Cyber Crime Investigator's Course (CCIC).

The 10-day course began in 2016 and gives participants the tools and skills to launch and run an advanced cyber investigation. The CCIC zeroes-in on cases where technology itself is the target, addressing crimes such as unauthorized use of computers, mischief to data and hacking.

"If officers have at least a general understanding of the concepts and technologies at play in their investigation, it helps them know what to seize, what to preserve, and to understand which cases require urgency," says Sgt. Nicolas Bernier, a senior cybercrime instructor at the CPC.

Cst. Scott Noseworthy, an RCMP investigator in Alberta, took the course earlier this year. He says it provided him with invaluable information and ultimately helped him deal with a ransomware attack — which is when a malicious software blocks access to a computer system until money is paid.

"After we did the course, we got a big file from a significant critical infrastructure partner, and we were able to respond to it more effectively because of what we learned," says Noseworthy. "Knowing what resources were available and how to co-ordinate with other police forces was a big advantage, not only to help us investigate, but to assist the victims."

TEACHING TECH

The amount of cybercrime in Canada is increasing, according to the latest RCMP statistics. In 2013, the force had about 4,400 reported incidents, up 40 per cent from 1,300 reported incidents in 2011. This spike in cybercrime has prompted the CPC to continually update and add new courses for international police officers and federal partners.

The CCIC is the newest cybercrime course offered through the Technological Crime Learning Institute (TCLI) at the CPC. The TCLI offers 14 specialized courses about digital forensics, technology and cybercrime geared for officers in the RCMP and other police agencies, along with civilian employees who are in intelligence or investigative positions.

These various programs, courses and workshops can lead police officers down one of two specialization paths — one for investigators looking to refine their techniques when handling Internet crimes, and one for those who want to specialize in digital forensics, or analyzing and extracting data from technological devices. All courses teach officers and civilians about how to enforce the law in this new technological era.

"Some of the traditional search-and-seize mentality applies but a lot of it is different with new technologies at play," says Bernier. "It's important that officers can hit the ground running and go in the right direction for these investigations because oftentimes evidence is ephemeral — it could be gone if you don't look for it right away."

A BETTER RESPONSE

The CCIC is taught by Sgt. Alex Baron, an RCMP senior cybercrime instructor. Baron says he brings in about 20 subject matter experts from the field to help him teach the course, including representatives from the Federal Bureau of Investigation in the United States.

"It's a good way to network — making contacts in the cyber world is very important," says Baron. "It's also important to get together because we need a common denominator for how cyber investigations proceed, especially between agencies. It's all about making things run more smoothly."

Baron and the other experts give participants real-life scenarios to work through, allowing the group to work together to gather information. In many cases, hackers leave a trail of digital breadcrumbs, so Baron teaches investigators how to follow the evidence and ask the right questions to solve a case.

After encountering several cybercrime cases since taking the course, Noseworthy can attest to the value of learning more about the intricacies of the Internet and the technologies involved.

"This course has made us more comfortable taking on cybercrime files, and made us better able to respond when we get those big cases," he says. "Given that these crimes are not only happening at a small scale — the $200 scams affecting your grandma — but also targeting major businesses and critical infrastructure across the country, it's now a basic skill for police to be able to deal with cybercrime files." ▪

MEANINGFUL EVIDENCE

NON-SPECIALISTS TRAINED TO TRIAGE DIGITAL DEVICES

By Deidre Seiden

Serge Gouin RCMP

The Digital Field Triage program trains front-line police officers to conduct an analysis of seized cellphones and computers at the scene.

Kathleen Vilac, a civilian member on the RCMP's Integrated Homicide Investigative Team (IHIT) in British Columbia, recalls one of the first cases she assisted as a member of the Digital Field Triage (DFT) Program.

It was 2012, and it was a shaken baby case. A computer was seized by IHIT and given to Vilac to search for evidence that could potentially further the investigation.

In the past, digital evidence would have been sent directly to a digital forensic specialist at the Technological Crime Unit (TCU) in the province. The specialists in the unit remember calling up the investigative teams they supported in the early days to let them know they were there to assist with correctly seizing and processing digital evidence.

"Back then, we had less work relative to the investigators that we had here," says S/Sgt. Clint Baker, the operations non-commissioned officer of the TCU in B.C. "But the pendulum has swung in the other direction. Now name any type of investigation and it could involve digital evidence."

When the use of cellphones and computers exploded, just about every seized device would be sent to the TCU, whether there was evidence on it or not. They had more work than they could handle.

"It doesn't do anybody any good if they send us something and it sits in the queue for two years and they can't get any meaningful evidence off of it in a timely fashion," says Baker. "We have to be relevant to the investigators."

A NEW APPROACH

To relieve the backlog, the TCU members developed the DFT program in 2009.

It was a new concept in the tech crime world. Typically, only digital forensic specialists were allowed to do forensics or analysis.

"We had to break down that barrier," says Sgt. Ben Hitchcock, who helped develop the program. "Our DFT members don't do analysis. They do extraction and create an observation report. That distinction is very important."

DFT members report on what they observe. "Anyone can see the fact that there's a child exploitation image on a computer," says Hitchcock. "However, they can't say how the image got there, how it was put on the computer, or when it was put onto the computer — all that information requires a digital evidence specialist to provide a higher level of analysis."

The program frees up the digital forensic specialists to focus on their work in their lab. A DFT member can determine if a digital device has evidence on it and if it needs to be sent to the TCU for further analysis.

"We only attend a search warrant now if there's an element of complex nature or if it's something that requires our expertise," says Sgt. Gerry Louie, the DFT program co-ordinator.

The DFT members also put evidence into the hands of the investigator faster.

"It's no longer stale post-mortem information," says Hitchcock. "Now the investigators are able to get emails, text messages — anything written on the computer — within hours of the arrest."

In the case of the shaken baby investigation, after Vilac extracted the data from the computer, she found evidence that the suspect had done an Internet search for infant cold and flu medication before the crime was committed. And post-offence, the suspect searched the term shaken baby syndrome and the effects of it.

"Anytime you find anything like that that can assist the investigators in pressing charges or as information to use during an interview with the suspect, it's very exciting and satisfying," says Vilac. "It's a 'Gotchya!' moment."

CROSS COUNTRY

The DFT program has trained more than 200 members across B.C. Interested front-line RCMP police officers and civilian members, like Vilac, can sign up for the five-day Digital Computer Field Triage training course or the four-day Digital Mobile Field Triage training course to become a member.

And the program has also gone national. The RCMP's National Division TCU uses it, as does the TCU in Ontario. It's also been implemented by the Ontario Provincial Police and supported by the Canadian Association of Chiefs of Police's e-Crime Committee.

"We have had interest from around the world as well," says Hitchcock. "Digital evidence is becoming *the* evidence in cases. And as a small parent unit, we can only do so much, but if we expand that to a second tier that has more people, we can do so much more." ■

CYBERCRIME ON THE FRONT LINE

BULLYING CASE PROMPTS CYBER WORKSHOP FOR POLICE

By Amelia Thatcher

Frontline police officers in Nova Scotia are now being trained to handle cybercrime cases, thanks to a new RCMP-led workshop. The single-day course gives officers the knowledge and tools to tackle any case with a cyber or technological element: from fraud and identity theft to online child exploitation and cyberbullying.

Run by the RCMP's Technological Crime Unit (TCU) in Nova Scotia, the Cybercrime Investigations Workshop explains what resources are available to RCMP and municipal police officers.

"The frontline guy might not be an expert, but they can refer members of the public to our specialized units," says Sgt. Royce MacRae, who's in charge of Nova Scotia's TCU. "It's making sure all police know what to do when that call comes to the office — to prevent tragedies like Rehtaeh Parsons."

In 2013, 17-year-old Rehtaeh Parsons committed suicide after months of intense online bullying in Cole Harbour, N.S., just outside of Halifax. Two years prior, the young teen was sexually assaulted by four boys at a party, who took a photo of the assault and circulated it via social media.

Parsons and her family went to police where a year-long investigation took place but no charges were laid. It wasn't until Parson's death that the case was reopened and two of the boys involved were charged and sentenced for child pornography-related offences.

"After the Rehtaeh Parsons case, there was an identified need for better education," says Cpl. Christian Hochhold, a member of the TCU who created the workshop. "Members in the front line just didn't know where to start."

THE RIGHT DIRECTION

The Cybercrime Investigations Workshop is a crash course in Internet and technology crimes for police officers of all skill levels. The single-day course starts with an introduction explaining what tech crime is, and how Nova Scotia's TCU can help with just about any investigation.

"The main takeaway is to call us," says Cst. Todd Bromley, a member of the TCU who instructs the workshop. "We can help with your domestics, your frauds, your thefts, your drug deals. Every crime has a technological component these days, and there's a lot we can bring to the table."

He says technology has changed the way crime is done, and that police need to keep up with the technology — and the laws and procedures that govern it — in order to do their job.

"When you do a drug bust, those dealers have computers that they use to get more clients, transfer money and keep track of their supplies," says Bromley. "Technology has enabled criminals to be better at what they do, but it can leave an electronic trail of evidence. We teach police how to get that evidence correctly so it can be used in an investigation."

PRESERVING EVIDENCE

Once officers are familiar with tech crimes, the RCMP's Legal Applications Support Team goes over recent case law related to seizing computer evidence, obtaining search warrants for electronic devices and any changes to legislation.

"We talk about a lot of the legal pitfalls with investigations," says Bromley. "There's a legal term called 'the fruits of the poisoned tree,' which means any piece of evidence that's been improperly processed, we lose. It's a minefield. You have to know the case law."

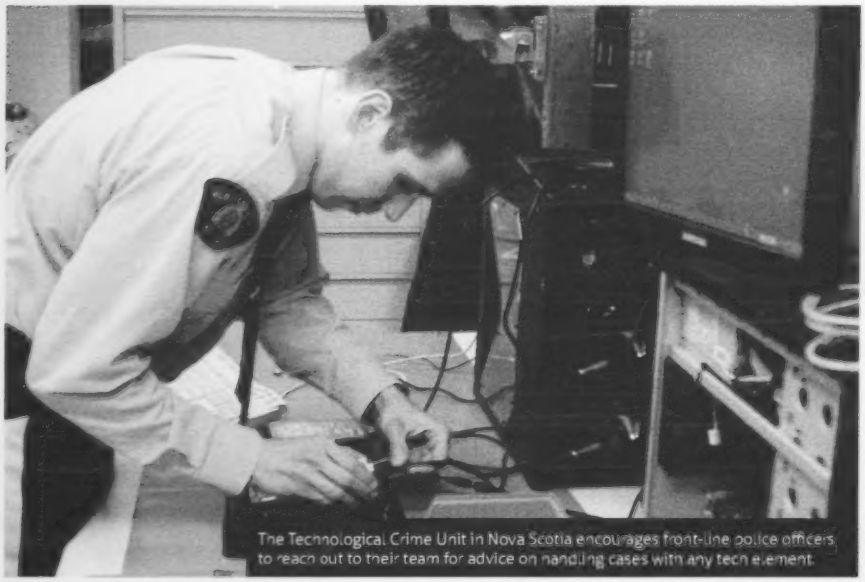
Then, the Internet Child Exploitation (ICE) team explains their role, encouraging all police officers to immediately contact an ICE unit if they come across a case involving a minor and sexually explicit material.

Bromley also explains how to properly seize electronic devices — he recommends taking out the SIM card or wrapping the device in tin foil to prevent it from accessing the Internet. He also goes over online services and social media platforms like Facebook, Twitter and Snapchat and how police can get information from them.

"It clears up some of the fog and mystery around these sorts of things, and puts it into an official step-by-step way," says Hochhold. "Since the workshops began, we've seen more investigations, better investigations and more evidence being properly seized and handled."

Hochhold hopes to have all police officers in Nova Scotia trained in the workshop by the end of 2017.

"At the end of the day, members, while inundated with cases, still have to take the time to know technologies," he says. "If you're frontline, you need to learn how to preserve digital evidence and data." ■



The Technological Crime Unit in Nova Scotia encourages front-line police officers to reach out to their team for advice on handling cases with any tech element.

RCMP

VISIONARY APPROACH

RCMP SEEKS SOFTWARE TO IDENTIFY CHILD EXPLOITATION

By Amelia Thatcher

When a new sexually explicit photo of a child is uploaded to the Internet, it's added to a vast collection of images that can be nearly impossible for police to find.

Until now.

The RCMP is turning to artificial intelligence technology to help investigators identify new online child exploitation images, and rescue at-risk children more quickly. Partnering with researchers from the University of Manitoba and the software firm Two Hat Security Ltd., the RCMP is hoping to use the new technology to triage cases.

According to Cpl. Dawn Morris-Little, an investigator at the RCMP-led National Child Exploitation Coordination Centre (NCECC) in Ottawa, prioritizing cases is a key part of her job.

"For every single one of our files, there's a child at the end of it," she says. "Images that look homemade or images that are unknown — those take priority because you don't know when it was created, and those children could still be at risk."

Since 2011, the RCMP has used similar software called PhotoDNA to help identify known and documented explicit photos. PhotoDNA works by converting photos into a hash code, which is like a unique fingerprint for each image. That hash code is added to a database, and if it's ever found again anywhere in the world — online or on a hard drive — PhotoDNA will flag it.

But with the rise of smartphones and tablets, creating new child exploitation content has never been easier. In 2016, the NCECC received 27,000 cases, almost double the number reported in 2015. This new content can't be identified by PhotoDNA, since it hasn't been added to its database yet.

"The numbers are only going up, so we need to be handling these cases in a much smarter way," says Sgt. Arnold Guerin, who works in the technology section of the Canadian Police Centre for Missing and Exploited Children (CPCMEC), which includes the NCECC. "New technology can provide us with tools to review cases in an automated way, and bubble up to the top the ones that need to be dealt with right away."

COMPUTER VISION

The artificial intelligence technology — called computer vision — is meant to mimic human vision. It uses algorithms to scan unknown photos and pick out the ones that have a high probability of being child exploitation.

"What would take weeks for an investigator would take the algorithm minutes or hours to scan," says Brad Leitch, head of product development at Two Hat Security. "The algorithm can eliminate the photos of trees and doughnuts and Eiffel Towers pretty successfully and put those high-probability, exploitative images at the top of the list so we can identify victims and make prosecutions more quickly."

Often, minutes matter in child exploitation investigations. Certain laws govern how long police can retain data, so the sooner an investigator can find evidence, the sooner they can lay charges.

"If we seize a hard drive that has 28 million photos, investigators need to go through all of them," says Guerin. "But how many are related to children? Can we narrow it down? That's where this project comes in, we can train the algorithm to recognize child exploitation."

Achieving 100 per cent accuracy with the algorithm isn't the goal — investigators will still have to go through all the material to make sure nothing is missed. This algorithm is meant to prioritize what police look at first, to make sure they're using their time and resources efficiently.

PROTECTING POLICE

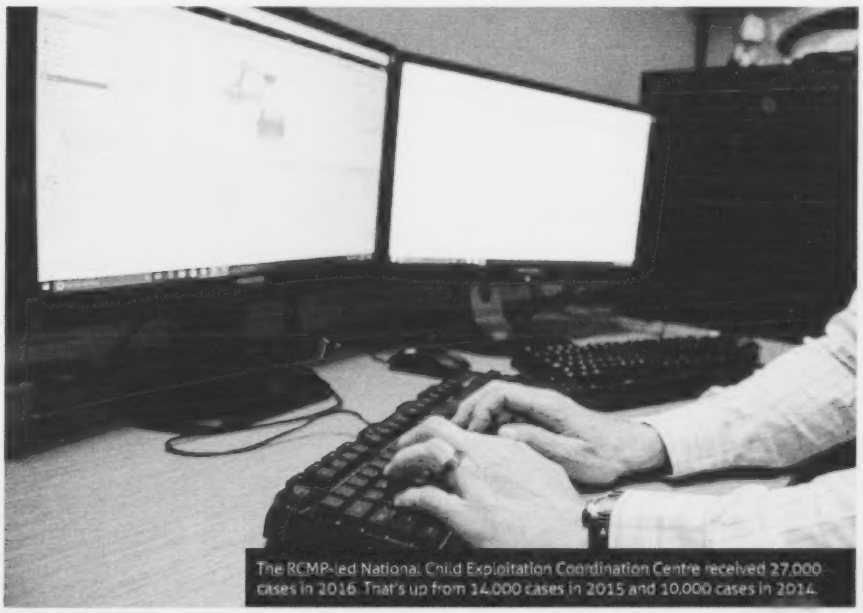
Along with reducing workload, technologies like PhotoDNA and computer vision can also help protect the health and wellness of investigators.

"We see images that no one wants to see, so maintaining our mental health is a priority," says Morris-Little. "Anything that takes the human element out of cases is going to reduce the risk of mental health injury to an investigator."

Guerin says technology like computer vision can act as a shield, sifting through material before it gets to an investigator.

The computer vision product is still in development, but Guerin hopes the RCMP will be able to use it later this year.

"If I could reduce the amount of toxicity officers have to endure every day, then I'm keeping them as healthy as possible, while also keeping more kids safe," he says. ■



Serge Gouin, RCMP

The RCMP-led National Child Exploitation Coordination Centre received 27,000 cases in 2016. That's up from 14,000 cases in 2015 and 10,000 cases in 2014.

HUNTING ONLINE PREDATORS

'SAVING MORE KIDS KEEPS ME GOING'

For the past five years, RCMP Cpl. Jared Clarke has worked as an investigator on Saskatchewan's Internet Child Exploitation (ICE) team. His expertise has helped crack numerous cases — rescuing dozens of children from their abusers both locally and abroad. Amelia Thatcher spoke to Clarke about how he keeps up with changing technologies to catch online predators.

RCMP Cpl. Jared Clarke is one of 11 police officers who work in Saskatchewan's Internet Child Exploitation Unit, which includes police from Saskatoon, Prince Albert and Regina.

Courtesy of Cpl. Jared Clarke, RCMP

HOW BIG OF A PROBLEM IS CHILD EXPLOITATION IN CANADA?

It's a huge problem. I get between 75 and 100 cases per year. One of my bigger files, the Russell Wolfe investigation in Saskatoon, Sask., has been on my desk since 2014. We discovered large-scale, hands-on abuse and found out that there were 14 local victims. In 2014, that was one of my 100 cases, but that single case took hundreds — if not thousands — of investigative hours.

WHAT TYPES OF INVESTIGATIONS DO YOU WORK ON?

There are both reactive and proactive investigations. Reactive files come from parents, detachments or the National Child Exploitation Coordination Centre in Ottawa. Proactive files are when we go on the Internet to search out child exploitation crimes. In peer-to-peer investigations, we're dealing directly with offenders who are making available or distributing child exploitation photos and videos. Using this material, we can track down the IP address [a location identifier assigned by the Internet service provider] where the material came from, contact the service provider, get the name and home address of the suspect, and eventually get a search warrant.

Another proactive way of finding child exploitation suspects is through online covert communication — that's what I specialize in. I can go online as a child and be lured by offenders, or I can pretend to be an offender talking to another offender. In both cases, it comes down to social engineering: the profile you create, the persona you emulate and the lingo you use.

WHAT CHALLENGES DO YOU FACE?

There are many. The rapid evolution of technology is a challenge, whether it's keeping up with the latest apps and software programs or the security systems and operating systems that encrypt data. Now, a lot of computers encrypt all their data when it's locked or powered off. Same goes for cellphones too. Another challenge is the content; it's getting worse and it's getting more graphic and extreme. You can hold a stiff upper lip all you want, but when you deal with that stuff, it sticks with you.

HOW OFTEN IS THIS TECHNOLOGY CHANGING?

Day-to-day and week-to-week. And it differs in different parts of the country — an app that's popular in Saskatchewan won't necessarily be used elsewhere. I was a fairly average computer user when I started working here. But as long as you're willing to learn and immerse yourself into it, the computer is a tool for us. Just like motorcycles are tools for traffic cops — you have to learn how to ride it to be good at your job.

WHAT DO OTHER FRONT-LINE OFFICERS NEED TO KNOW ABOUT THESE CASES?

People ask: 'How do you tell who the bad guy is walking down the street?' And I tell them there's no mould or profile for an offender. We've had every kind of person from the basement dweller to teachers, business professionals and unfortunately other police officers. I tell other officers to get a hold of an ICE unit early to get direction. They're very complex investigations and there are steps that need to be taken when seizing computers and devices. If it's not done properly, you can lose that data. And once it's gone, there's slim chance of getting it back.

WHAT KEEPS YOU DOING THIS TYPE OF WORK?

Our ultimate goal is to save kids. It's both the best day ever and the worst day ever when you get a case where live abuse has occurred — it's terrible because it's happening, but great because you're going to be able to stop it and get kids out of a bad spot. So with that, it's the most rewarding work I've done in 12 years of policing. I've had a number of files where we've identified live local victims; I just got another one on my desk right now with the potential to save a number of kids overseas. So, even though I'm sitting at the bottom of this mountain looking up, the thought of being able to save more kids, that's what keeps me going. ■

just THE FACTS

AUTO THEFT

Stealing vehicles is a lucrative business for criminals in Canada. As a result, auto theft is an unfortunate reality that many Canadians deal with each year. It crosses all boundaries of criminals from petty break and enters to grand theft auto, and after more than 10 years of decline, auto theft is once again on the rise.

Each year, automobile thefts cost Canadians close to $1 billion, says the Insurance Bureau of Canada. This can be broken down to $542 million for insurers to fix or replace stolen vehicles, $250 million in police, health care and court system costs, and the rest for correctional services.

According to the Insurance Bureau of Canada, on average, a car is stolen every seven minutes in Canada.

It's estimated that about 40 people die and 65 people are injured as a direct result of auto theft every year.

Hamilton Police Service says the most common location for vehicle thefts are large, anonymous parking lots like the ones at shopping malls, automotive dealerships, residential driveways and unlocked garages.

Criminals steal vehicles for several reasons, including to sell abroad, often with their vehicle identification number (VIN) intact. These vehicles are immediately packed and shipped to be sold for more than their original market value.

Domestically, vehicles are given a false VIN and sold to unsuspecting consumers or they're sold for parts. Some cars are stolen simply to joyride or get somewhere, while others are stolen to commit another crime.

Vehicles that are stolen to commit another crime are often recovered — abandoned and damaged — within 48 hours of being stolen.

The Insurance Bureau of Canada says an experienced thief can steal a car in as little as 30 seconds.

In B.C., a unit was created to deal specifically with auto theft. Twenty-two specialized police auto theft investigators from seven police forces in the Greater Vancouver area, including the RCMP, make up the Integrated Municipal Provincial Auto Crime Team (IMPACT).

IMPACT uses bait cars — cars that are owned by the police and are intended to be stolen — to track the location, speed and direction of travel of the vehicle, which is tracked by police dispatchers. The dispatcher co-ordinates the police response and disables the car with the click of a mouse, which allows for the quick arrest of the thieves.

Motor vehicle theft increased in Calgary to 7,684 thefts in 2015 from 4,499 incidents in 2014. The growing number of thefts, including auto theft, has pushed the police-reported crime rate in Alberta up by 30 per cent.

The increase in Alberta has contributed to the first increase in the national police-reported crime rate in 12 years, says Statistics Canada. In 2015, there were 78,849 cars reported stolen in Canada. That's a six per cent increase over the previous year.

In Coquitlam, B.C., after cracking an identity theft ring, RCMP investigators found that one out of three of the stolen identity documents like insurance papers, driver's licenses and passports being used to create fraudulent ID could be traced back to vehicle theft files.

To avoid being an easy target for car theft, the RCMP recommends that car owners lock vehicle doors and keep windows rolled up, park in the garage and lock it, park in well-lit and well-populated areas, take keys, garage openers and vehicle registration papers out of the vehicle when you leave it, and check on your vehicle regularly even if it's not being used.

The RCMP recommends that you don't do the following: leave spare keys in the car or leave spare keys in visible spots in your home, leave the car running, leave any purses, backpacks or other items unattended in the vehicle — even in the trunk. Make sure the vehicle has an immobilizer. If it doesn't, consider having one installed or using an anti-theft device.

— Compiled by Deidre Seiden

CRUMBS OF DIGITAL DATA

DATA ANALYST MAKES SENSE OF PHONE CALLS

When it comes to technology and how it affects policing, RCMP communications data analyst Robert Aboumitri has a determination to innovate. On his prompting, the RCMP created the Communications Data Analysis Team (CDAT), the first unit of its kind in Canada, which Aboumitri leads. Deidre Seiden spoke to him about what mobile phone data can reveal to police and how it can inform investigations.

WHY DID YOU PUSH FOR THE CREATION OF CDAT?

Early in 2008, I was deployed by the RCMP to Lebanon to assist in the investigation of the ex-Prime Minister who was assassinated. We had a lot of phone data — every single phone call in the country of Lebanon in a database.

We were pioneering analytical techniques to exploit and get results out of that data. And when I came back to Canada, I started to preach to the RCMP that there's a lot more in phone data than meets the eye — everybody has a unique digital print.

WHAT IS COMMUNICATIONS DATA?

Essentially it's metadata that we obtain, legally and lawfully, from various providers, such as Rogers. It's data about communication. It's not the content of the data that we receive and examine, it's the details of the data.

So when it comes to communications metadata, it's information about the phone calls themselves. It's not just about user of phone A contacted user of phone B anymore. It's the device number, their contacts, routing [cell sites], the date, time and duration, the serial number of the handset, etc. If a suspect used multiple phone numbers [several SIM cards] on that same device, we could identify that.

We make sense of that, create visuals to explain it and create a comprehensive report for the investigative team.

HOW DO YOU MAKE SENSE OF WHAT YOU COLLECT?

We normalize it and organize it in a way to turn it from data to information. A date on its own means nothing. When I turn a date into the day of the week, I can find patterns of usage that repeat themselves, say on Sunday. When I turn a date into a month, I can see which month a suspect's visited a general area the most. Now I've turned data into information.

Once I have information and once I have multiple layers of information, then we start to understand what happened after and then what does that mean. That's when we produce intelligence and provide recommendations.

IT SOUNDS LIKE A FORM OF SURVEILLANCE.

In a way, but in the past, which is impossible to undertake in any other way. That's the beauty of it. If you've made a mistake in the past using the phone, you can't undo that mistake. For example, we can show that a phone was in the general area of a crime when a crime was committed, and we can take that one step further and show that for the 24 months before that they were never in that area.

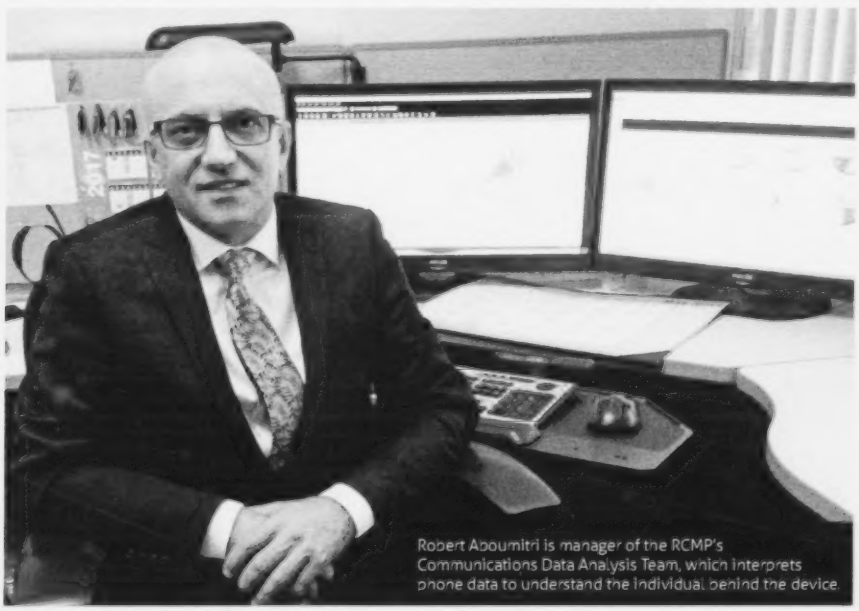
Fingerprints can be wiped clean, and clothes burned, but digital data from phone records can't be erased by the criminal.

HOW DOES YOUR UNIT HELP INVESTIGATORS?

In this digital age, we're leaving crumbs of digital data behind everywhere we go and in everything that we do. Modern mobile devices are ubiquitous. They go to sleep with us, speak to our friends, and access the websites we're interested in. They do everything that we like to do and go with us everywhere we go. And they're our camera, our alarm clock, our calendar, our web-browsing device — cellphones are the Swiss Army knife of technology.

The frequent usage of these devices really turns them into a tracker in the hand of the user. And if you know how to leverage that information and make sense of it, there's so much you can do with it. If investigators aren't leveraging this to their advantage, they're missing out.

We provide a perspective that no other field can provide. We can corroborate a lot of evidentiary information that otherwise couldn't be corroborated through any other means. It gives us a bit of an advantage that we otherwise don't have. Since we live in an age where digital devices are omnipresent, we need to leverage that to enhance our ability to conduct our investigative work in particular and police work in general. ■



Courtesy of Robert Aboumitri, RCMP

Robert Aboumitri is manager of the RCMP's Communications Data Analysis Team, which interprets phone data to understand the individual behind the device.

FITNESS OVER AGE

JOINING THE RCMP AS A SECOND CAREER

By Amelia Thatcher

It was in the midst of cancer treatments that Cst. Ellen Ruf decided to apply to the RCMP. The single mother of three had worked in an office for most of her life, often taking on two jobs to keep her family afloat. Now having faced a life-changing illness, 50-year-old Ruf decided she wanted to make a bigger mark on the world.

"At that point, I knew there was more for me. It made me realize life is really short," says Ruf. "I wanted to be able to help people and make the world a better place for my kids."

As soon as she was well again, Ruf set her sights on the RCMP. With encouragement from her partner — an RCMP officer — she began the task of applying to the force. She put in the paperwork and immediately began getting back into physical shape.

"I've been told my best qualities are my hard work and determination," says Ruf, who just completed her on-the-job police field coaching in Kamsack, Sask. "Being a little bit older has actually helped me through this process. I have life experiences and I know how to talk to different types of people."

LIFE EXPERIENCE

Much like Ruf, Cst. David Andrews decided to join the RCMP later in life, at age 55. Before applying, Andrews worked as a photographer and wilderness guide in the Canadian Arctic. There, he noticed the integral role the RCMP played in northern communities like Grise Fiord, Nunavut.

"That's what initially inspired me to apply — that combination of being exposed to Mounties in the North and the possibility of using photography working in the RCMP," he says. "I've learned that policing is a lot different than what I imagined. It's challenging, interesting and the work is more diverse."

In many ways, Andrews says his previous work experience has helped him become a better police officer. Managing group dynamics, being responsible for people's safety and learning to be respectful of others' circumstances are just a few of the skills Andrews has transferred from being a photographer and adventure guide to policing.

"I learned how to get along with a diverse range of people, and those interpersonal skills have proved valuable," says Andrews. "Those experiences helped define who I am as a person, and those skills are applicable to policing because serving the public is a huge part of our job."

Andrews says his experience has already helped him deal with some tough policing situations at his first posting in Grande Prairie, Alta.

"During my first week, we brought an intoxicated guy off the street and a couple of my colleagues commented on the fact that I was able to develop a rapport with him very easily," says Andrews. "He was being obstinate with other members, so I started a conversation with him. He became amicable and began to work with us instead of against us."

FITNESS MATTERS

Joining the RCMP as a second career isn't unusual — the average age of a cadet at Depot, the RCMP's national training centre, is 28.

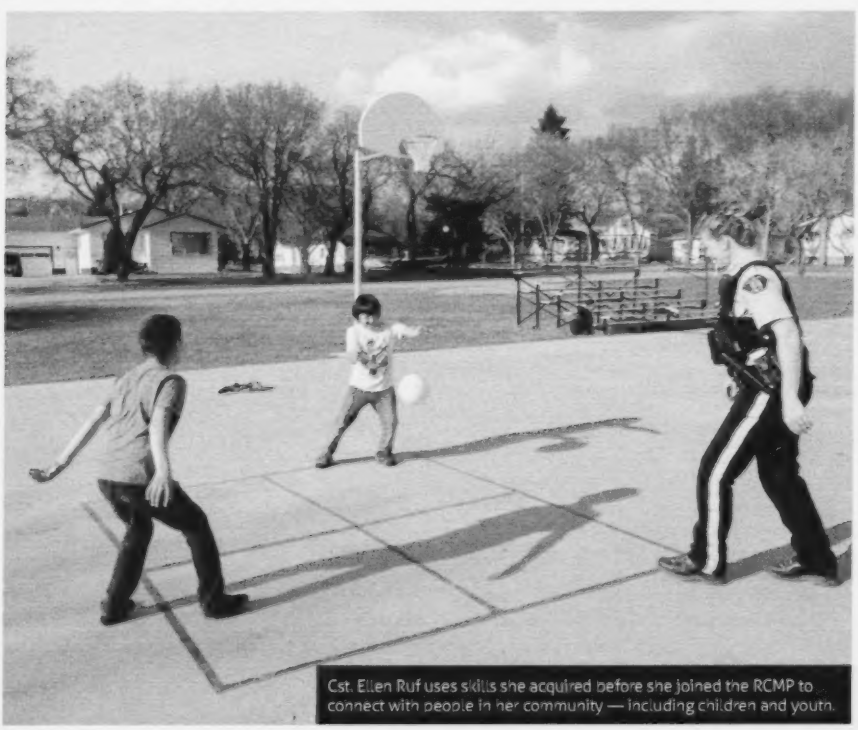
Besides a minimum age of 19, there are no other age restrictions when it comes to applying to the force: any person who meets the RCMP's recruiting qualifications can apply. That being said, older cadets like Ruf and Andrews are still few and far between. Over the last 10 years, only 24 cadets over the age of 50 have graduated from RCMP training.

But Depot fitness facilitator Leslie Frei says age isn't a good indicator of how well a cadet will perform during police training.

"If you're coming to Depot unfit, whether you're 20, 40 or 60, it's going to be a struggle," says Frei, who's been teaching cadets for 18 years. "But if you are fit, some people in their 40s and 50s far surpass our younger cadets because they have that experience to draw from. They know their body."

Frei remembers Andrews surpassing many of his peers at Depot. He excelled in speed and running, coming out at the top of his class despite being the oldest cadet. Likewise, Ruf performed in the top 10 per cent of all cadets at Depot for strength and endurance.

"When you set your mind to something, it's never too late," says Ruf. "I'm proof of that." ■



Cst. Ellen Ruf uses skills she acquired before she joined the RCMP to connect with people in her community — including children and youth.

Cpl. Jennifer Smith, RCMP

OFF-ROAD RULES

STOPPING UNSAFE ATV USE IN ITS TRACKS

By Amelia Thatcher

In Newfoundland and Labrador, all-terrain vehicles (ATVs) aren't just a mode of transportation — they're a way of life. Off-road trails intersect forests and fields, connecting houses, neighbourhoods and communities.

For youth, ATVs can provide a source of freedom and entertainment, especially in rural communities like Holyrood, N.L. But oftentimes, young drivers don't fully understand all the rules of the road.

"Here, we get a lot of complaints about youth driving [ATVs] on the road, without helmets or not following the proper regulations," says S/Sgt. Boyd Merrill, commander of the Holyrood RCMP detachment. "Catching these young people, giving them fines and releasing them wasn't working, so we had to be more proactive."

After a surge of ATV complaints in Holyrood last summer, Merrill consulted the town, emergency services and local schools. With input from youth, he created the TYRE program — Teaching Youth Responsibility through Education.

The two-hour program teaches ATV safety to youth aged 12 to 17. In it, Merrill discusses the laws and regulations, safe driving techniques and the penalties and fines for not following the law.

"It gives young ATV users the knowledge they need to make the right decisions so that reckless behaviour is diminished," says Merrill. "They learn to do things more safely so they aren't getting hurt, receiving complaints or damaging property."

TARGETING YOUTH

The first session ran last October in Holyrood and drew approximately 40 youth, along with parents and members of the community. The demand was so high, Merrill ran a second session in December, and also presented the program in Ferryland, N.L., a neighbouring community.

"The most important thing was to target the right age of youth," says Sgt. Frank Flynn, an officer in-charge at the Ferryland detachment. "It was good to get the legalese out of the way to make sure everyone understood it in layman's terms. The laws aren't always written for the average person to understand."

In Holyrood, N.L., an RCMP-led program called TYRE — Teaching Youth Responsibility through Education — targets unsafe ATV driving by youth.

Coun. Roger Myette

After finishing the program, the teens got TYRE stickers to put on the back of their ATVs and helmets. The sticker lets the RCMP know that the youth have been educated, fostering more positive interactions with police.

Since the TYRE program was delivered last fall in Holyrood, the number of ATV complaints involving young people has dropped. Merrill says in April, his detachment got its first complaint in nine months.

"We saw a massive drop in not only complaints, but dangerous behaviour in general during our routine patrols," says Merrill. "As the weather gets warmer, there will inevitably be complaints, but we hope they'll be on a much smaller scale this year."

A RURAL ISSUE

In Newfoundland and Labrador, youth can start driving ATVs when they turn 14, but it has to be below a certain size and they have to be with an adult. After the age of 16, they can drive any size of ATV without supervision. Additionally, all drivers are required to wear a helmet and goggles or a face shield, and they have to stick to trails rather than paved roads.

The TYRE program goes into the intricacies of these rules, making them easy for everyone to understand. According to Roger Myette, a Holyrood city councillor and avid ATV user, this is the first time the RCMP has held an event aimed at ATV safety, rather than bicycles or cars.

"These kids are good kids, but when they get on the road they think they're invincible," says Myette. "It was great to educate them and let them know what can happen if they aren't careful."

When the RCMP asked Myette for input in the TYRE program, he posed the question to his 15-year-old son.

"The first thing my son said was, 'Dad, I need stories I can relate to, if you give me stats and numbers, I'm going to zone out,' " says Myette.

The RCMP listened and included those real-life stories and consequences. "And the kids really retained the information because of it."

After the TYRE session last fall, Merrill says there's been a demand from adults in the Holyrood area who want a similar education program.

"The program is just as valuable to adults as it is to young people," says Merrill. "It's a new approach to something that's been an issue in rural parts of every province in the country." ■

LATEST RESEARCH IN LAW ENFORCEMENT

The following are excerpts from recent research related to justice and law enforcement and reflect the views and opinions of the authors and not necessarily those of the organizations for which they work.

Compiled by Deidre Seiden

EVALUATION SUMMARY OF THE ATLANTIC YOUTH INCLUSION PROGRAM

By Danièle Laliberté

The Youth Inclusion Program (YIP) is a geographically based program aimed at reducing crime in specific neighbourhoods with high rates of crime by targeting 50 youth aged 13 to 16 who are most at risk of offending. This complex and intensive program is based on individualized action plans developed for each youth and targets specific risk factors.

Specifically, YIP aims to increase protective factors, school attendance and school performance, while decreasing risk factors, youth offending and the number of youth in the criminal justice system. Three YIP projects implemented in the Atlantic region with funding from Public Safety Canada participated in an impact evaluation conducted by a contractor: Northside YIP in North Sydney, N.S. (January 2010 – June 2013); Seeds of Change YIP in Spryfield, N.S. (September 2010 – November 2012) and ONE Change YIP in St. John, N.B. (April 2010 – January 2014).

A total of 257 youth were admitted. In general, the three YIP sites were very successful in reaching their intended targeted groups. Consistent with the idea that a YIP should be placed in a high risk area, neighbourhood was among the top two risk factors across all three sites. Lifestyle, thinking and behaviour, school and education, and family and personal relationships were among the top factors in at least one site.

In-depth interviews with school staff, police and representatives from various social service organizations confirmed that the YIPs were reaching high-risk and appropriate youth; these stakeholders believed that the program was better received by those youth whose risk level was somewhat more moderate, and should not target youth who were too entrenched in the criminal justice system. A minimum target of five hours of intervention per week was planned (between five to 10 hours).

The fact that some youth were involved in the YIP intervention before being officially admitted in the ONE Change site had made it difficult to determine the extent to which the outcomes could be attributed to the intervention. This challenge illustrates how important it is to appropriately align program recruitment, implementation and the outcomes being measured. Another key finding is that youth who had participated more intensely in the program derived greater benefit from the YIP intervention. An indication that the expected short-term outcomes of the YIP intervention were reached was that 67 per cent of all participants decreased their total risk level based on the ONSET score. It's notable that some progress was also made regarding intermediary outcomes related to school-related indicators.

There was also a decrease in criminal offending for several YIP participants, particularly in the Northside and the Seeds of Change sites, where respectively 59 per cent and 50 per cent of the youth decreased suspected/charged contacts with the police between the end of the YIP and the end of Year 2 post-program. Twenty-five per cent of the Northside businesses saw a decrease in criminal incidents during program implementation. The majority of Northside business representatives expressed the belief that the program was somewhat or entirely responsible for decreasing youth anti-social behaviour.

READ THE FULL REPORT:
publicsafety.gc.ca

HIDDEN CONSEQUENCES: THE IMPACT OF INCARCERATION ON DEPENDENT CHILDREN

By Eric Martin

Family members of incarcerated individuals are often referred to as "hidden victims" — victims of the criminal justice system who are neither acknowledged nor given a platform to be heard. Children whose parents are involved in the criminal justice system, in particular, face a host of challenges and difficulties: psychological strain, anti-social behaviour, suspension or expulsion from school, economic hardship and criminal activity. It's difficult to predict how a child will fare when a parent is intermittently or continually incarcerated, and research findings on these children's risk factors are mixed.

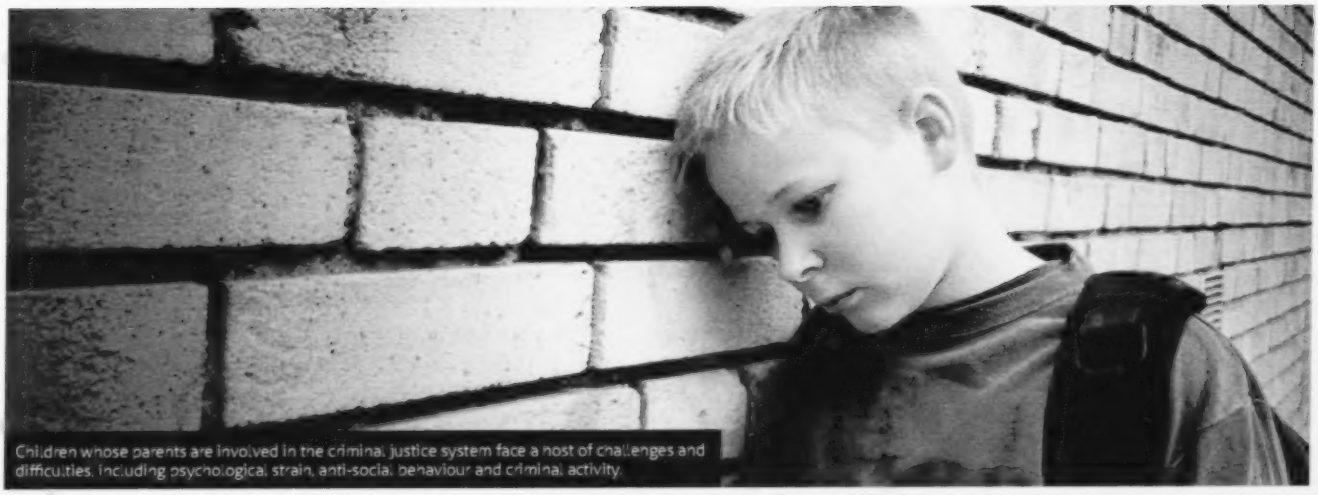
However, research suggests that the strength or weakness of the parent-child bond and the quality of the child and family's social support system play significant roles in the child's ability to overcome challenges and succeed in life. Therefore, it's critical that correctional practitioners develop strong partnerships with law enforcement, public schools and child welfare agencies to understand the unique dynamics of the family in question and try to ensure a safety net for the child and successful re-entry for the incarcerated parent.

This article summarizes the range of risk factors facing children of incarcerated parents. It also cautions against universal policy solutions that seek to address these risk factors but don't take into account the child's unique needs, the child's relationship with the incarcerated parent and alternative support systems.

Although each case is unique and each child responds differently, research has established that a parent's incarceration poses several threats to a child's emotional, physical, educational and financial well-being.

Law enforcement and child welfare practitioners are often involved with the child before the correctional system is involved with the parent, so enhanced and streamlined communication between the various government entities could maximize the potential to provide the child whatever support is available.

For example, NIJ-funded research on crossover youth cited the "one family, one judge" model, which combines cases in child welfare and juvenile justice to provide a streamlined and consistent approach to services for the child and family. If law enforcement, child welfare, educational and correctional practitioners can share information on the child and family experiencing



Children whose parents are involved in the criminal justice system face a host of challenges and difficulties, including psychological strain, anti-social behaviour and criminal activity.

parental incarceration, it would be more likely that the child would benefit from early intervention if he or she appears to be at risk for sustained deprivation, loss of educational attainment or criminal activity. Such a partnership would also benefit correctional practitioners and re-entry managers, who would have better information on the child's situation and prior relationship with the incarcerated parent, which seems to be critical for the child's welfare.

Given these considerations, it appears that enhancing communication between corrections practitioners and other service providers is a good way to ensure a safety net for the child and facilitate a successful re-entry for the incarcerated parent.

READ THE FULL REPORT:
nij.gov

VIOLENT EXTREMISM IN AUSTRALIA: AN OVERVIEW

This overview by Shandon Harris-Hogan

Australia is one of the most culturally and linguistically diverse nations in the world. Although a wide range of backgrounds and beliefs are present within the Australian community, the nation has experienced a relatively peaceful recent history. While violent extremism is considered more or less a permanent feature of western societies, the threat to the Australian community from violent extremism has been comparatively small. However, that threat has remained persistent for a long period of time.

Although most have not been successful, in excess of 150 planned acts of violent extremism have occurred in Australia since Second World War. In this paper, the various forms of violent extremism that have impacted Australia over time are briefly chronicled and analysis is provided as to how the phenomenon contrasts with other broadly comparable countries.

Groups involved in international political or independence struggles are commonly termed ethno-nationalists. For example, between 1967 and 1973, the Australian wing of the Croatian Revolutionary Brotherhood was responsible for 10 separate bombings in Australia.

There's a long history of far-right activity in Australia and a number of violent incidents have also occurred post-2000. For instance, an organized campaign of violence was planned in Perth in 2004, with Jack Van Tongeren and four associates convicted of conspiring to firebomb four Chinese restaurants. Tongeren had previously led the Australian Nationalists' Movement in the 1980s and the attacks were intended to coincide with the launch of his book on the group.

Violence dedicated to a specific cause, such as environmental protection or anti-abortion, is known as issue-oriented violence. For the most part, criminal behaviour associated with a specific issue is disruptive and largely involves using threatening behaviour and criminal damage to promote a particular group or message.

In recent times, the primary violent extremist threat to Australia has come from jihadism. While acts of jihadist violence are often justified by the perpetrators using selectively literal interpretations of traditional Islamic texts, the motivation for such violence is predominantly political.

Post-2003, Australia's domestic jihadist events have shifted from being funded and directed by international organizations, to homegrown self-starting plots. This shift, which was not consistent with comparable countries internationally, was predominantly due to the removal of key facilitators with significant overseas connections from within the Australian jihadist network.

This threat has been heightened by the recent increase in the number of Australians travelling to fight in Syria and Iraq, and the documented connection between fighting in overseas insurgencies (as well as participation in training camps) and the perpetration of acts of violent extremism in Western countries.

However, this isn't the only potential threat. A historical presence of far-right extremists in Australia and dramatic attacks conducted internationally by individuals such as Wade Michael Page, Anders Breivik and David Copeland have demonstrated the potential for far-right violence. Further, issue-oriented and ethno-nationalist groups continue to operate in Australia and are likely to remain as an ongoing security concern into the future. ■

READ THE FULL REPORT:
aic.gov.au/publications

OVERCOMING ADVERSITY

OFFICER SHARES STORY TO HELP OTHERS

By Deidre Seiden

Cst. Dwayne Pardy has a unique ability to connect with the residents of each community he works in, which isn't an easy feat as a relief officer in Canada's North.

On an almost monthly basis, the RCMP member rotates in and out of communities to cover temporary vacancies at local detachments.

In addition to responding to emergencies, he gets to know the residents, often on a first-name basis. He has also taught the Drug Abuse Resistance Education program in northern schools.

Norma Hickey, a nurse in Paulatuk, N.W.T., has witnessed the little things Pardy does on and off duty. She recalls one example where she watched as Pardy helped an elder down the stairs of the local store.

"He cares about people," says Norma Hickey. "I've seen Dwayne in several communities and he leaves a lasting impression everywhere he goes. People are always asking after him when he's not there."

One secret in his bag of tricks is for the kids. "I always bring candy when I go to a new community," says Pardy.

The other is a secret he shared for the first time in 2007 with a group of children in foster care when he was working in Summerside, P.E.I.

It's the story of his childhood.

A CHILD'S TRAGEDY

When Pardy was 10, he and a friend ran their snowmobile straight into the back of RCMP Cst. Keith Atwin's snowmobile in Happy Valley-Goose Bay, N.L. The impact from that would shape his life.

Pardy was going through a difficult time — his father had recently died from cancer and his mother was also sick with the disease.

But Atwin, who drove both children home, must have picked up on it.

"Looking back on it, it was obvious my mother was quite ill," says Pardy. "I don't know how it came to be, but I didn't get into trouble."

After that, Atwin started to drop by the house to visit. The two forged a strong friendship.

"It got to the point where I was spending more time with him than I was at home," says Pardy.

It was at Atwin's house that he received the life-changing news that his mother had died.

FOSTER CARE

Pardy, now orphaned, was taken away from his home, his brothers and his sisters — and Atwin — and was sent to live with a foster family in Grand Prairie, Alta.

Life in Alberta was far from ideal. Pardy suffered physical abuse at the hands of one of his foster fathers — to the point where Pardy couldn't recognize his own battered reflection in the mirror.

He left to live with his friend's older sister and her boyfriend. With them, he felt at home with people who cared about him. But after a disagreement, he took to the streets, dropped out of school and ended up living in an old junkyard van.

"I was afraid of two things during that time," says Pardy. "That I was going to freeze to death or end up getting crushed in the scrapyard."

Pardy knew he needed to do something.

He got back in touch with social services, got a place of his own and a job. He eventually found and reconnected with his siblings and moved back to Labrador, where he got married and became a father.

Pardy didn't always think he was good enough to join the RCMP. But it was still in the back of his mind — to follow in Atwin's footsteps.

After unsuccessfully applying once, he reconnected with Atwin, who urged him to apply again.

In 2005, at the age of 35, Pardy became a Mountie. A short time later, Pardy learned that Atwin had died. And it was then that the apprentice became the teacher.

He still recalls the look of disbelief on the foster kids faces when he revealed that he was a police officer.

"I started the talk in my street clothes, then left the room and returned in my RCMP uniform," says Pardy. "As good as the talk was for them to see they can succeed, it was good for me, too."

It was the first time he shared his story publicly. And he's been sharing it ever since.

"As police officers, we very often deal with people who come from unfortunate situations," says Cst. Lyndon Martin, from the Paulatuk detachment.

"I have a great respect for Cst. Pardy because he has a better insight into what a lot of people go through."

Pardy's message for young people is that they can succeed no matter what life throws at them as long as they work hard for it.

"I'll tell my story 1,000 times if it helps one kid." ■

Cst. Dwayne Pardy's personal history helps him to connect with people, from youth to elders, in the communities he polices.

Cst. Kenji Welch, RCMP